Success Probability of Multiple/Multidimensional Linear Cryptanalysis Under General Key Randomisation Hypotheses

Subhabrata Samajder*and Palash Sarkar
Applied Statistics Unit
Indian Statistical Institute
203, B.T.Road, Kolkata, India - 700108.
subhabrata.samajder@gmail.com, palash@isical.ac.in

Abstract

This work considers statistical analysis of attacks on block ciphers using several linear approximations. A general and unified approach is adopted. To this end, the general key randomisation hypotheses for multidimensional and multiple linear cryptanalysis are introduced. Expressions for the success probability in terms of the data complexity and the advantage are obtained using the general key randomisation hypotheses for both multidimensional and multiple linear cryptanalysis and under the settings where the plaintexts are sampled with or without replacement. Particularising to standard/adjusted key randomisation hypotheses gives rise to success probabilities in 16 different cases out of which in only five cases expressions for success probabilities have been previously reported. Even in these five cases, the expressions for success probabilities that we obtain are more general than what was previously obtained. A crucial step in the analysis is the derivation of the distributions of the underlying test statistics. While we carry out the analysis formally to the extent possible, there are certain inherently heuristic assumptions that need to be made. In contrast to previous works which have implicitly made such assumptions, we carefully highlight these and discuss why they are unavoidable. Finally, we provide a complete characterisation of the dependence of the success probability on the data complexity.

Keywords: multidimensional linear cryptanalysis, multiple linear cryptanalysis, chi-squared distribution, success probability, data complexity, advantage.

1 Introduction

Linear cryptanalysis for block ciphers was introduced by Matsui in [21]. Matsui's work spurred a great deal of research and considered several aspects of linear cryptanalysis. At a broad level, the attacks are of two types. The goal of one type of attack is to recover (a subset of the bits of) the secret key and such attacks are called key recovery attacks. A different and weaker type of attack seeks to only distinguish the output of a block cipher from uniform random bits. Such attacks are called distinguishing attacks. In this work, we will be concerned only with key recovery attacks.

At a broad level, linear cryptanalysis proceeds in the following manner. A careful study of the block cipher results in one or more linear approximations. During the data collection phase, N plaintexts $P_1, \ldots, P_N$ are chosen and the corresponding ciphertexts under a secret but, fixed key are obtained. The key recovery algorithm is applied to the obtained plaintext-ciphertext pairs and the output is a list of possible values of the (partial) key. An attack is said to be successful if the correct value of the key is in the output list. For an attack, the success probability is denoted by P_S; the data complexity is N; and the attack has an advantage a, if the size of

*Financial support from the R. C. Bose Center for Cryptology and Security, Indian Statistical Institute, Kolkata, India.

the output list is 2^{-a} times the total number of (partial) keys. The goal of a statistical analysis of such a key recovery attack is to obtain a relation between P_S, N and a.

A formal statistical treatment of linear cryptanalysis has the following aspects.

Multiple versus multidimensional linear cryptanalysis: One issue is whether a single linear approximation is available or, whether several such linear approximations are available. In the later case, analysis is of two types depending on whether the several linear approximations can be considered independent or not. If the analysis is under the independent assumption, then the attack is often called multiple linear cryptanalysis whereas if the independence assumption is not made, then the attack is often called multidimensional linear cryptanalysis.

Sampling with or without replacement: For the attack, plaintexts $P_1, \ldots, P_N$ are randomly sampled and the corresponding ciphertexts are obtained. One issue is whether the plaintexts are considered to be sampled uniformly at random with replacement or, whether they are considered to be sampled uniformly at random without replacement.

Key randomisation hypothesis: The linear approximations hold with certain probabilities. The basis for the attack is that the probability corresponding to the right key is different from the probability corresponding to a wrong key. In the standard key randomisation hypothesis, the probabilities corresponding to both the right and the wrong key are assumed to be fixed. The adjusted or, revised (as termed in [7]) key randomisation hypothesis assumes that the probabilities themselves are random variables.

Our Contributions

In this work, we consider the scenario when several linear approximations are available. Our goal is to express P_S in terms of N and a in each of the above mentioned settings. Table 1 lists all the 16 possible cases that can arise and in each case mentions whether the case has been previously considered in the literature or whether it is new. If a case has occurred earlier, then the corresponding reference is provided and the last column provides the section number of this work where an expression for P_S can be found. We observe that out of the 16 possible cases, only 6 cases have been considered earlier and in 5 of these cases expressions for success probabilities have been reported.

We provide a general and unified treatment to the extent possible and the 16 different cases are obtained as special cases of the general treatment. The route that we take is similar to the route taken in [27] for single linear cryptanalysis.

Linear cryptanalysis identifies a target sub-key and attempts to obtain the correct value of the target sub-key in time less than an exhaustive search over all possible values of the whole secret key. At a broad level, linear cryptanalysis applies a statistical test to each possible value of the target sub-key. Section 2 provides an overview of linear cryptanalysis and identifies the test statistic that is to be used. The test statistic is parameterised by the choice of the target sub-key and the distribution of the test statistic depends on whether the choice is right or wrong. For a statistical analysis, it is required to obtain the distributions of the test statistic under both the right and the wrong choices of the target sub-key.

The literature provides two approaches for analysing success probability, namely the order statistics based approach and the hypothesis testing based approach. Assuming certain forms of the distributions of the test statistic for the right and the wrong key choices, Section 3 obtains expressions for P_S following both the order statistic and the hypothesis testing based approaches. Certain problems with the order statistics based approach which were earlier pointed out in [25, 27] are briefly summarised. It is shown that if some approximations are applied to the expression for P_S obtained using the hypothesis testing based approach then one obtains the expression for P_S obtained using the order statistics based approach. Since such approximations do not seem

type	samp.	RKRH	WKRH	new	previous P_S	new P_S
md	wr	std	std	no [16]	[16]	Section 7.1.1
		std	adj	yes	–	Section 7.1.2
		adj	std	no [17]	–	Section 7.1.3
		adj	adj	no [7]	[7]	Section 7.1.4
	wor	std	std	yes	–	Section 7.1.1
		std	adj	yes	–	Section 7.1.2
		adj	std	yes	–	Section 7.1.3
		adj	adj	no [7]	[7]	Section 7.1.4
m	wr	std	std	yes	–	Section 7.2.1
		std	adj	yes	–	Section 7.2.2
		adj	std	yes	–	Section 7.2.3
		adj	adj	no [7]	[7]	Section 7.2.4
	wor	std	std	yes	–	Section 7.2.1
		std	adj	yes	–	Section 7.2.2
		adj	std	yes	–	Section 7.2.3
		adj	adj	no [7]	[7]	Section 7.2.4

Table 1: Here md (resp. m) denotes multidimensional (resp. multiple) linear cryptanalysis; wr (resp. wor) denotes sampling with (resp. without) replacement. RKRH (resp. WKRH) is an abbreviation for right (resp. wrong) key randomisation hypothesis; std (resp. adj) denotes whether the standard (resp. adjusted) key randomisation hypothesis is considered.

to be necessary, the rest of the paper follows the expression for P_S obtained using the hypothesis testing based approach.

The literature has separately considered the standard and the adjusted key randomisation hypotheses. In Section 4, we discuss the existing hypotheses and point out some heuristic assumptions in their formulation that have been implicitly made in the literature. We propose a general right key randomisation hypothesis and a general wrong key randomisation hypothesis and show that the existing key randomisation hypotheses can be obtained as special cases of these two general hypotheses.

Section 5 takes up the crucial task of obtaining the distributions of the test statistic. These distributions are obtained under the general right and wrong key randomisation hypotheses. The cases of multidimensional and multiple linear cryptanalysis and that of sampling with and without replacement are treated separately. For obtaining the distributions, we proceed formally to the extent possible. The derivation of the distributions, however, requires several heuristic assumptions. We carefully identify these heuristics and discuss why these cannot be replaced by formal analysis. Distributions of the test statistic under the right and wrong key have been obtained earlier for particular cases. We remark that heuristic assumptions similar to those that we identify have also been implicitly made in previous works.

Section 6 obtains expressions for P_S under the general key randomisation hypotheses for the cases of multidimensional/multiple linear cryptanalysis. It turns out that a compact expression for P_S can be provided covering both sampling with and without replacement. The expressions for P_S are obtained by combining the distributions of the test statistics obtained in Section 5 with the expression for P_S obtained in Section 3 following the hypothesis testing framework.

Expressions for P_S for the 16 possible cases mentioned in Table 1 are obtained in Section 6. These expressions are obtained by specialising the general key randomisation hypotheses to either the standard or the adjusted key randomisation hypothesis for both right and wrong key choices. As mentioned above, expressions for P_S

are obtained for the first time in 11 out of the 16 possible cases. In the remaining five cases, making several approximations to the expressions for P_S that are obtained in this work, it is possible to obtain the expressions for P_S obtained in earlier works. Since such approximations do not seem to be necessary, even in the remaining five cases, the expressions for P_S are more general than what was previously known.

Intuitively, one may assume that for a fixed value of the advantage a, the success probability is a monotonic increasing function of the data complexity N. On the other hand, the expressions for P_S show a complicated dependence on N. Section 8 closely analyses the dependence of the success probability on N. To do this, the general and compact expressions for P_S obtained in Section 6 are used. A complete characterisation of the nature of monotonicity of P_S on N is obtained. This characterisation is then specialised to the particular cases of standard/adjusted key randomisation hypothesis and sampling with/without replacement. To the best of our knowledge, no previous work in the literature has carried out such an extensive analysis of the monotonic behaviour of P_S with respect to N.

Previous and Related Works

Linear cryptanalysis was introduced by Matsui [21]. An earlier work [30] had considered linear approximation in the context of an attack on S-boxes of FEAL. The initial work of Matsui [21] considered using a single linear approximation. A subsequent work [22] by Matsui himself showed how to improve linear cryptanalysis if two linear approximations are available. Independently, Kaliski and Robshaw [20] also showed that the availability of several linear approximations with certain restrictions leads to an improved attack. Both the attacks [22, 20] considered the linear approximations to be independent. Further analysis under the independence assumption of the linear approximations was later done in [4]. Murphy [23] observed that the independence assumption may not be valid.

A series of papers [2, 3, 19] carried out a systematic investigation of multiple linear cryptanalysis where the linear approximations are not necessarily independent. The motivation of these works was to analyse and obtain optimal distinguishers to distinguish between two distributions. This was done using the framework of hypothesis testing. Several important techniques, including the log-likelihood ratio test, were successfully developed to build optimal distinguishers.

Matsui's original work [21] employed a ranking approach to key recovery attacks. A subsequent work by Selçuk [28] proposed a formal statistical treatment of this approach using the methodology of order statistics. The work by Selçuk proved to be quite influential and the order statistics based approach was adopted in a number of later papers [16, 5]. Selçuk's work required an asymptotic result on normal approximation of order statistic. A concrete error bound on the normal approximation was obtained in [25] and several problematic issues with the order statistics approach were pointed out. The alternative hypothesis testing based approach to analysing key recovery attacks was suggested in [25] and has been subsequently used in [7].

Treatment of key recovery attacks for multidimensional linear cryptanalysis without requiring any independence assumption on the linear approximations was carried out by Hermelin, Cho and Nyberg [16]. This work followed the order statistic based approach of Selçuk [28] and analysis of the same setting using the hypothesis testing based approach was done in [25].

The standard wrong key randomisation hypothesis was formally introduced by Harpes et al. in [15]. The first work to consider the adjusted key randomisation hypothesis was by Bogdanov and Tischhauser [11]. This was in the setting of single linear cryptanalysis. The formulation of the adjusted key randomisation hypothesis was based on an earlier work on statistical properties of uniform random permutation by Daemen and Rijmen [14]. A later work on adjusted key randomisation hypotheses for single linear approximation is by Ashur et al. [1]. A general and unified treatment of success probability under general key randomisation hypotheses for single linear cryptanalysis has been done in [27].

Extension of the adjusted right key randomisation hypothesis from single to multidimensional linear cryptanalysis was considered in Huang et al. [17]. The work did not provide an expression for the success probability.

Out of the 16 possible cases listed in Table 1, four cases were considered by Blondeau and Nyberg in [7] and expressions for P_S obtained in these cases. As mentioned earlier, these expressions are less general than the ones that we obtain in the present work.

A related line of work [10, 12, 9, 8] considers zero correlation attacks. The notion of sampling without replacement was first considered in the setting of multidimensional zero correlation attack [9]. In this paper, we do not consider zero correlation attacks.

Much of the analysis in the context of linear cryptanalysis is based on approximations where the errors in the approximations are not known. A more rigorous approach has been advocated in [24] where such approximations are avoided and instead rigorous upper bounds on the data complexity are obtained. A test statistic whose analysis avoids approximations and also avoids some of the problems associated with the generally used test statistics has been proposed in [26].

2 Linear Cryptanalysis

Let the function $E : \{0,1\}^k \times \{0,1\}^n \mapsto \{0,1\}^n$ denote a block cipher such that for each $K \in \{0,1\}^k$, $E_K(\cdot) \stackrel{\Delta}{=} E(K,\cdot)$ is a bijection from $\{0,1\}^n$ to itself. Here K is called the secret key. The n-bit input to the block cipher is called the plaintext and n-bit output of the block cipher is called the ciphertext.

In general, block cipher constructions involve a simple round function parametrised by round key iterated over several rounds. The round functions are bijections of $\{0,1\}^n$. Round keys are produced by applying an expansion function, called the key scheduling algorithm, to the secret key K. Denote the round keys by $k^{(0)}, k^{(1)}, \ldots$ and round functions by $R^{(0)}_{k^{(0)}}, R^{(1)}_{k^{(1)}}, \ldots$. Also, let $K^{(i)}$ denote the concatenation of the first i round keys, i.e., $K^{(i)} = k^{(0)} \,||\, \cdots \,||\, k^{(i-1)}$ and $E^{(i)}_{K^{(i)}}$ denote the composition of the first i round functions, i.e.,

$$E^{(1)}_{K^{(1)}} = R^{(0)}_{k^{(0)}}; \quad E^{(i)}_{K^{(i)}} = R^{(i-1)}_{k^{(i-1)}} \circ \cdots \circ R^{(0)}_{k^{(0)}} = R^{(i-1)}_{k^{(i-1)}} \circ E^{(i-1)}_{k^{(i-1)}}; i \geq 1.$$

A reduced round cryptanalysis of a block cipher targets $r+1$ rounds of the total number of rounds proposed by the block cipher design. For a plaintext P, we denote by C the output after $r+1$ rounds, i.e., $C = E^{(r+1)}_{K^{(r+1)}}(P)$, and by B the output after r rounds, i.e, $B = E^{(r)}_{K^{(r)}}(P)$ and $C = R^{(r)}_{k^{(r)}}(B)$. Throughout this paper, we will be assuming an attack on the first $r+1$ rounds of an iterated block cipher with $r+1$ rounds.

Linear approximations: Block cipher cryptanalysis starts off with a detailed analysis of the block cipher. This results in one or possibly more relations between the plaintext P, the input to the last round B and possibly the expanded key $K^{(r)}$. In case of linear cryptanalysis these relations are linear in nature and are of the following form:

$$\langle \Gamma^{(i)}_P, P\rangle \oplus \langle \Gamma^{(i)}_B, B\rangle = \langle \Gamma^{(i)}_K, K^{(r)}\rangle; \quad i = 1, 2, \ldots, \ell;$$

where $\Gamma^{(i)}_P, \Gamma^{(i)}_B \in \{0,1\}^n$ and $\Gamma^{(i)}_{K^{(r)}} \in \{0,1\}^{nr}$ denote the plaintext mask, the mask to the input of the last round and the key mask. A linear relation of the form above is called a linear approximation of the block cipher. These linear approximations usually hold with some probability which is taken over random choices of the plaintext P. In case $\ell > 1$, it is required to work with the corresponding joint distribution. Obtaining such relations and their joint distribution is a non-trivial task and requires a lot of ingenuity and experience. They form the basis on which the statistical analysis of block ciphers are built. In this work we will only consider $\ell > 1$. There are two cases.

Multiple linear cryptanalysis: The linear approximations are assumed to be independent.

Multidimensional linear cryptanalysis: The linear approximations are not assumed to be independent.

Let

$$L_i \stackrel{\Delta}{=} \langle \Gamma_P^{(i)}, P \rangle \oplus \langle \Gamma_B^{(i)}, B \rangle; \text{ for } i = 1, 2, \ldots, \ell. \tag{1}$$

Inner key bits: Let

$$z_i = \langle \Gamma_K^{(i)}, K^{(r)} \rangle; \quad i = 1, \ldots, \ell.$$

Note that for a fixed but unknown key $K^{(r)}$, z_i represents a single unknown bit. Denote by $z = (z_1, \ldots, z_\ell)$ the collection of the bits arising in this manner. Since, all the ℓ key masks $\Gamma_K^{(1)}, \ldots, \Gamma_K^{(\ell)}$ are known, the tuple z is determined only by the unknown but fixed $K^{(r)}$. Hence, there is no randomness either of $K^{(r)}$ or z. We call z as the inner key bits.

Target sub-key bits: Any linear relation between P and B of the form (1) usually involves only a subset of the bits of B. When $\ell > 1$, several relations between P and B are known. In such cases, it is required to consider the subset of the bits of B which covers all the relations. In order to obtain these bits from the ciphertext C it is required to (partially) decrypt C by one round. This involves a subset of the bits of the last round key $k^{(r)}$. We call this subset of bits of $k^{(r)}$ as the target sub-key.

Recall that the ciphertext C is obtained by encrypting P using the secret key K. Let κ^* denote the value of the target sub-key corresponding to the secret key K. The goal of linear cryptanalysis is then to find the correct value of the target sub-key κ^* using the ℓ linear approximations and their (joint or marginal) distributions.

Denote the size of the target sub-key by m. In other words, these m key bits are sufficient to partially decrypt C by one round and obtain the bits of B involved in any of the ℓ linear approximations. There are 2^m possible choices of the target sub-key out of which only one correct. The purpose of the attack is to identify the correct key.

Joint distribution parametrised by inner key bits: Let the plaintext P be chosen uniformly at random from $\{0,1\}^n$; C be the ciphertext obtained after encrypting with the secret key K; and B the result of partial decryption of C with a choice κ of the target sub-key. The random variable B depends on the choice κ used to invert C partially by one round whereas the ciphertext C depends on the correct choice κ^* of the target sub-key and hence so does B. So the random variable L_i depends on both κ and κ^*. Hence, to emphasise this dependence we write $L_{\kappa,\kappa^*,i}$ for $\kappa \neq \kappa^*$ and simply write $L_{\kappa^*,i}$ for $\kappa = \kappa^*$. Define the random variables X_{κ,κ^*} and X_{κ^*} as follows:

$$X_{\kappa,\kappa^*} = (L_{\kappa,\kappa^*,1}, \ldots, L_{\kappa,\kappa^*,\ell}) \quad \text{and} \quad X_{\kappa^*,i} = (L_{\kappa^*,1}, \ldots, L_{\kappa^*,\ell}).$$

Also, define the joint distribution of the random variables $X_{\kappa,\kappa^*} \oplus z$ and $X_{\kappa^*} \oplus z$ to be

$$q_{\kappa,\kappa^*,z}(\eta) = \Pr[L_{\kappa,\kappa^*,1} = \eta_1 \oplus z_1, \ldots, L_{\kappa,\kappa^*,\ell} = \eta_\ell \oplus z_\ell] = \frac{1}{2^\ell} + \epsilon_{\kappa,\kappa^*,\eta}(z); \tag{2}$$

and

$$p_{\kappa^*,z}(\eta) = \Pr[L_{\kappa^*,1} = \eta_1 \oplus z_1, \ldots, L_{\kappa^*,\ell} = \eta_\ell \oplus z_\ell] = \frac{1}{2^\ell} + \epsilon_{\kappa^*,\eta}(z) \tag{3}$$

respectively, where $-1/2^\ell \leq \epsilon_{\kappa,\kappa^*,\eta}(z), \epsilon_{\kappa^*,\eta}(z) \leq 1 - 1/2^\ell$. Denote by $\tilde{q}_{\kappa,\kappa^*,z} = (q_{\kappa,\kappa^*,z}(0), q_{\kappa,\kappa^*,z}(1), \ldots, q_{\kappa,\kappa^*,z}(2^\ell - 1))$ and $\tilde{p}_{\kappa^*,z} = (p_{\kappa^*,z}(0), p_{\kappa^*,z}(1), \ldots, p_{\kappa^*,z}(2^\ell - 1))$ the corresponding probability distributions, where the integers $\{0, 1, \ldots, 2^\ell - 1\}$ are identified with the set $\{0,1\}^\ell$. For each choice of z, we obtain a different but related distribution. Let $z' = z \oplus \beta$ for some $\beta \in \{0,1\}^\ell$. It is easy to verify that $\epsilon_{\kappa,\kappa^*,\eta}(z') = \epsilon_{\kappa,\kappa^*,\eta\oplus\beta}(z)$ and $\epsilon_{\kappa^*,\eta}(z') = \epsilon_{\kappa^*,\eta\oplus\beta}(z)$, which implies that

$$q_{\kappa,\kappa^*,z\oplus\beta}(\eta) = q_{\kappa,\kappa^*,z}(\eta \oplus \beta) \quad \text{and} \quad p_{\kappa^*,z\oplus\beta}(\eta) = p_{\kappa^*,z}(\eta \oplus \beta). \tag{4}$$

Let $\tilde{p}_{\kappa^*}$ and $\tilde{q}_{\kappa,\kappa^*}$ denote the probability distributions $\tilde{p}_{\kappa^*,0^\ell}$ and $\tilde{q}_{\kappa,\kappa^*,0^\ell}$, respectively. We write

$$\tilde{q}_{\kappa,\kappa^*} = (q_{\kappa,\kappa^*}(0), \ldots, q_{\kappa,\kappa^*}(2^\ell - 1)) \quad \text{and} \quad \tilde{p}_{\kappa^*} = (p_{\kappa^*}(0), \ldots, p_{\kappa^*}(2^\ell - 1)). \tag{5}$$

For $i = 1, \ldots, \ell$, define

$$q_{\kappa,\kappa^*,i} = \Pr[L_{\kappa,\kappa^*,i} = 1] \quad \text{and} \quad p_{\kappa^*,i} = \Pr[L_{\kappa^*,i} = 1]. \tag{6}$$

Statistical model of the attack: Let $P_1, \ldots, P_N$, with $N \leq 2^n$, be N plaintexts chosen randomly from the set $\{0,1\}^n$ of all possible plaintexts and assume that these N plaintexts follow some distribution over the set $\{0,1\}^n$. Also assume that the adversary possess N plaintext-ciphertext pairs $(P_j, C_j); j = 1, 2, \ldots, N$, such that $C_j = E_K(P_j)$ for some fixed key K. Given N plaintext-ciphertext pairs, the goal of the adversary is then to find κ^* in time faster than a brute force search on all possible keys of the block cipher.

For each choice κ of the target sub-key it is possible for the attacker to partially decrypt each C_j by one round to obtain $B_{\kappa,j}; j = 1, 2, \ldots, N$. Note that $B_{\kappa,j}$ is dependent on κ even though C_j may not be. For $\kappa = \kappa^*$, C_j clearly depends on κ, whereas for the $\kappa \neq \kappa^*$, C_j has no relationship with κ. Define,

$$\begin{aligned} L_{\kappa,i,j} &= \langle \Gamma_P^{(i)}, P_j \rangle \oplus \langle \Gamma_B^{(i)}, B_{\kappa,j} \rangle, & (7)\\ X_{\kappa,z,j} &= (L_{\kappa,1,j} \oplus z_1, \ldots, L_{\kappa,\ell,j} \oplus z_\ell), & (8)\\ Q_{\kappa,z,\eta} &= \#\{j \in \{1,2,\ldots,N\} : X_{\kappa,z,j} = \eta\}, & (9) \end{aligned}$$

where $\kappa \in \{0, 1, 2, \ldots, 2^m - 1\}; z_1, \ldots, z_\ell \in \{0,1\}; j = 1, 2, \ldots, N;\ i = 1, 2, \ldots, \ell$. Note that

$$\sum_{\eta \in \{0,1\}^\ell} Q_{\kappa,z,\eta} = N. \tag{10}$$

The condition $X_{\kappa,z\oplus\beta,j} = \eta$ is written as

$$\begin{aligned} (L_{\kappa,1,j} \oplus z_1 \oplus \beta_1, \ldots, L_{\kappa,\ell,j} \oplus z_\ell \oplus \beta_\ell) &= \eta \\ \Rightarrow (L_{\kappa,1,j} \oplus z_1, \ldots, L_{\kappa,\ell,j} \oplus z_\ell \oplus \beta_\ell) &= \eta \oplus \beta \\ \Rightarrow X_{\kappa,z,j} &= \eta \oplus \beta, \end{aligned}$$

where $\beta = (\beta_1, \ldots, \beta_\ell)$. Therefore,

$$Q_{\kappa,z\oplus\beta,\eta} = Q_{\kappa,z,\eta\oplus\beta}. \tag{11}$$

The variable $X_{\kappa,z,j}$ is determined by the pair (P_j, C_j), the choice κ of the target sub-key and the choice z of the inner key bits. Recall that C_j depends upon K and hence upon κ^* which implies that $X_{\kappa,z,j}$ also depends upon κ^* through C_j. The randomness of $X_{\kappa,z,j}$ arises from the randomness in P_j and also possibly from the randomness of the previous $P_1, \ldots, P_{j-1}$. In fact it depends on how $P_1, \ldots, P_N$ are sampled from $\{0,1\}^n$. Therefore $\Pr[X_{\kappa,z,j} = \eta]$ potentially depends upon the following quantities:

z	: the choice of the inner key bits;
$p_{\kappa^*,z}(\eta)$ or $p_{\kappa,\kappa^*,z}(\eta)$	: the probabilities of linear approximations as given in (2) and (3).
j	: the index determining the pair (P_j, C_j).

This models a general scenario which captures a possible dependence on the index j. The dependence on j will be determined by the joint distribution of the plaintexts $P_1, \ldots, P_N$. In the case that $P_1, \ldots, P_N$ are independent and uniformly distributed, $\Pr[X_{\kappa,z,j} = \eta]$ does not depend on j. On the other hand, suppose that $P_1, \ldots, P_N$ are sampled without replacement. In such a scenario, $\Pr[X_{\kappa,z,j} = \eta]$ does depend on j.

Test statistic for multidimensional linear cryptanalysis: For each choice κ of the target sub-key and the inner key bits z, let $T_{\kappa,z} \equiv T(X_{\kappa,z,1}, \ldots, X_{\kappa,z,N})$ denote the test statistic.

$$T_{\kappa,z} = \sum_{\eta \in \{0,1\}^\ell} \frac{\left(Q_{\kappa,z,\eta} - N2^{-\ell}\right)^2}{N2^{-\ell}}.$$

Then

$$\begin{aligned} T_{\kappa,z\oplus\beta} &= \sum_{\eta \in \{0,1\}^\ell} \frac{\left(Q_{\kappa,z\oplus\beta,\eta} - N2^{-\ell}\right)^2}{N2^{-\ell}} \\ &= \sum_{\eta \in \{0,1\}^\ell} \frac{\left(Q_{\kappa,z,\eta\oplus\beta} - N2^{-\ell}\right)^2}{N2^{-\ell}}; \quad \text{[By (11)]} \\ &= \sum_{\eta\oplus\beta \in \{0,1\}^\ell} \frac{\left(Q_{\kappa,z,\eta} - N2^{-\ell}\right)^2}{N2^{-\ell}} = \sum_{\eta \in \{0,1\}^\ell} \frac{\left(Q_{\kappa,z,\eta} - N2^{-\ell}\right)^2}{N2^{-\ell}} = T_{\kappa,z}. \end{aligned}$$

So $T_{\kappa,z}$ is independent of z. Therefore it is sufficient to consider $z = 0^\ell$. To simplify notation, we will write T_κ instead of $T_{\kappa,z}$. Therefore,

$$T_\kappa = \sum_{\eta \in \{0,1\}^\ell} \frac{\left(Q_{\kappa,\eta} - N2^{-\ell}\right)^2}{N2^{-\ell}}. \tag{12}$$

There are 2^m choices of κ, which give rise to 2^m random variables T_κ. The distribution of T_κ depends on whether κ is correct or incorrect. For statistical analysis of an attack, it is required to obtain the distribution of T_κ under both correct and incorrect choices of the target sub-key. Later we will consider this issue in more details.

Remark: Recall that, since there is no randomness over $K^{(r)}$, the bits z_i's also have no randomness even though they are unknown. Therefore the distribution of $L_{\kappa,i,j} \oplus z_i$ is completely determined by the distribution of $L_{\kappa,i,j}$.

Test statistic for multiple linear cryptanalysis: In this case, the linear approximations are assumed to be independent. As a result, it is possible to define a simpler test statistic. For each choice κ of the target sub-key and inner key bits $z = (z_1, \ldots, z_\ell)$, let

$$Y_{\kappa,z,i,j} = L_{\kappa,i,j} \oplus z_i \quad \text{and} \quad Y_{\kappa,z,i} = \sum_{j=1}^{N} Y_{\kappa,z,i,j},$$

where $i = 1, \ldots, \ell$ and $j = 1, \ldots, N$. For $z = 0^\ell$, we simply write $Y_{\kappa,i,j}$ and $Y_{\kappa,i}$ instead of $Y_{\kappa,z,i,j}$ and $Y_{\kappa,z,i}$ respectively. Let $\beta = (\beta_1, \ldots, \beta_\ell)$. If $\beta_i = 0$, then $Y_{\kappa,z\oplus\beta,i,j} = Y_{\kappa,z,i}$; if $\beta_i = 1$, then $Y_{\kappa,z\oplus\beta,i,j} = 1 - (L_{\kappa,i,j} \oplus z_i)$ and $Y_{\kappa,z\oplus\beta,i} = N - Y_{\kappa,z,i}$. Consequently, for any β, $(Y_{\kappa,z,i} - N/2)^2 = (Y_{\kappa,z\oplus\beta,i} - N/2)^2$. Let $T_{\kappa,z} \equiv T(X_{\kappa,z,1}, \ldots, X_{\kappa,z,N})$ denote the test statistic

$$T_{\kappa,z} = \sum_{i=1}^{\ell} \frac{(Y_{\kappa,z,i} - N/2)^2}{N/4}.$$

For $\beta = (\beta_1, \ldots, \beta_\ell)$,

$$T_{\kappa,z\oplus\beta} = \sum_{i=1}^{\ell} \frac{(Y_{\kappa,z\oplus\beta,i} - N/2)^2}{N/4} = \sum_{i=1}^{\ell} \frac{(Y_{\kappa,z,i} - N/2)^2}{N/4} = T_{\kappa,z}.$$

So, $T_{\kappa,z}$ is independent of β and as in the multidimensional case, it is sufficient to consider $z = 0^\ell$. We will write T_κ instead of $T_{\kappa,0^\ell}$ and this is defined as follows.

$$T_\kappa \;=\; \sum_{i=1}^{\ell} \frac{(Y_{\kappa,i} - N/2)^2}{N/4}. \tag{13}$$

Success probability: An attack will produce a set (or a list) of candidate values of the target sub-key. The attack is considered successful if the correct value of the target sub-key κ^* is in the output set. The probability of this event is called the success probability of the attack.

Advantage: An attack is said to have advantage a if the size of the set of candidate values of the target sub-key is equal to 2^{m-a}. In other words, a fraction 2^{-a} portion of the possible 2^m values of the target sub-key is produced by the attack.

Data complexity: The number N of plaintext-ciphertext pairs required for an attack is called the data complexity of the attack. Clearly, N depends on the success probability P_S and the advantage a. One of the goals of a statistical analysis is to be able to obtain a closed form relation between N, P_S and a.

Additional Notation

Capacity: Let $\tilde{p} = (p_0, \ldots, p_{2^\ell - 1})$ be a probability distribution over $\{0,1\}^\ell$. The multidimensional capacity $C^{(\mathrm{md})}(\tilde{p})$ is defined as

$$C^{(\mathrm{md})}(\tilde{p}) \;=\; 2^\ell \sum_{i=0}^{2^\ell - 1} (p_i - 2^{-\ell})^2 = 2^\ell \sum_{i=0}^{2^\ell - 1} \epsilon_i^2 \tag{14}$$

where $\epsilon = p_i - 2^{-\ell}$. When $\tilde{p}$ is clear from the context, we will simply write $C^{(\mathrm{md})}$ instead of $C^{(\mathrm{md})}(\tilde{p})$.

There is a corresponding notion [7] which is useful in the case of multiple linear cryptanalysis. Let $\tilde{p} = (p_1, \ldots, p_\ell)$ be such that $0 \le p_i \le 1$, $i = 1, \ldots, \ell$; then $C^{(\mathrm{m})}(\tilde{p})$ is defined to be

$$C^{(\mathrm{m})}(\tilde{p}) \;=\; \sum_{i=1}^{\ell} 4\,(p_i - 1/2)^2 = \sum_{i=1}^{\ell} 4\epsilon_i^2 \tag{15}$$

where $\epsilon = p_i - 1/2$. When $\tilde{p}$ is clear from the context, we will simply write $C^{(\mathrm{m})}$ instead of $C^{(\mathrm{m})}(\tilde{p})$.

Normal distribution: By $\mathcal{N}(\mu, \sigma^2)$ we will denote the normal distribution with mean μ and variance σ^2. The density function of $\mathcal{N}(\mu, \sigma^2)$ will be denoted by $\mathfrak{f}(x; \mu, \sigma^2)$. The density function of the standard normal will be denoted by $\phi(x)$ while the distribution function of the standard normal will be denoted by $\Phi(x)$.

Chi-squared distribution: The probability density function of a central chi-square distribution with ν degrees of freedom will be denoted by $\chi^2_\nu(x)$ and its corresponding cumulative density function will be denoted by $\Psi_\nu(x)$. The density function of a non-central chi-square distribution with ν degrees of freedom and a non-centrality parameter δ will be denoted by $\chi^2_{\nu,\delta}(x)$ and its cumulative density function will be denoted by $\Psi_{\nu,\delta}(x)$.

3 Two Approaches for Deriving Success Probability

The test statistic for the multidimensional case is given in (12) and for the multiple case is given in (13). To obtain the success probability of an attack it is required to obtain the corresponding distributions of T_κ for the two scenarios $\kappa = \kappa^*$ and $\kappa \neq \kappa^*$. Suppose that the following holds.

$$T_{\kappa^*} \sim \mathcal{N}(\mu_0, \sigma_0^2); \qquad T_\kappa/\omega \sim \chi^2_\nu, \quad \kappa \neq \kappa^*, \tag{16}$$

where $\omega > 0$ is a constant.

In this section, we consider the derivation of the success probability in terms of μ_0, σ_0^2, ν and ω. Later, we will see how to obtain μ_0, σ_0^2, ν and ω. In particular, we will see that δ depends on N whereas ν depends on the number of linear approximations ℓ.

From (16), there are two approaches to deriving success probability which we discuss below.

3.1 Order Statistics Based Analysis

This approach is based on a ranking methodology used originally by Matsui [21] and later formalised by Selçuk [28]. The idea is the following. There are 2^m random variables T_κ corresponding to the 2^m possible values of the target sub-key. Suppose the variables are denoted as $T_0, \ldots, T_{2^m-1}$ and assume that T_0 corresponds to the choice of the correct target sub-key κ^*. Let $T_{(1)}, \ldots, T_{(2^m-1)}$ be the order statistics of $T_1, \ldots, T_{2^m-1}$, i.e., $T_{(1)}, \ldots, T_{(2^m-1)}$ is the ascending order sort of $T_1, \ldots, T_{2^m-1}$. So, the event corresponding to a successful attack with a-bit advantage is $T_0 > T_{(2^m q)}$, where $q = 1 - 2^{-a}$.

Using a well known result on order statistics, the distribution of $T_{(2^m q)}$ can be assumed to approximately follow $\mathcal{N}(\mu_q, \sigma_q^2)$ where $\mu_q = \Psi_\nu^{-1}(1 - 2^{-a-1})$ and $\sigma_q^2 = \frac{2^{-(m+a)}(1-2^{-a})}{\chi^2_\nu(\mu_q)}$. For the asymptotic version of the result refer to [31] and for a concrete error bound refer to [25]. Further assuming that T_0 and $T_{(2^m q)}$ are independent the success probability P_S can be approximated in the following manner.

$$\begin{aligned} P_S &= \Pr[T_0 > T_{(2^m q)}] = \Pr[T_0 - T_{(2^m q)} > 0] \\ &\approx 1 - \Phi\left(\frac{-(\mu_0 - \mu_q)}{\sqrt{\sigma_0^2 + \sigma_q^2}}\right) = \Phi\left(\frac{\mu_0 - \mu_q}{\sqrt{\sigma_0^2 + \sigma_q^2}}\right) \\ &= \Phi\left(\frac{\mu_0 - \Psi_\nu^{-1}(1 - 2^{-a-1})}{\sqrt{\sigma_0^2 + \sigma_q^2}}\right); \end{aligned} \tag{17}$$

where $\mu_0 = E[T_0] = E[T_{\kappa^*}] = \nu + \delta$ and $\sigma_0^2 = E[(T_0 - \mu_0)^2] = E[(T_{\kappa^*} - \mu_0)^2] = 2(\nu + 2\delta)$.

Some criticisms: The order statistics based approach is crucially dependent on the normal approximation of the distribution of the order statistics. A key observation is that the order statistics result is applied to 2^m random variables and for the result to be applied even in an asymptotic context, it is necessary that 2^m is sufficiently large. In [25] a close analysis of the hypothesis of the theorem and the error bound in the concrete setting showed that both m and $m - a$ must be large. In particular, to ensure that the approximation error is at most around 10^{-3}, it is required that $m - a$ should be at least around 20 bits. Since a is the advantage of the attack, the applicability of the order statistics based analysis for attacks with high advantage is not clear.

For the analysis to be meaningful one needs to make two further independence assumptions which were implicitly used by Selçuk in [28]. This issue has been pointed out in [27].

1. The hypothesis of the result on the normal approximation of order statistics requires the random variables $T_1, T_2, \ldots, T_{2^m-1}$ to be *independent* and identically distributed. The randomness of all of these random variables arise from the randomness of $P_1, \ldots, P_N$ and so these random variables are certainly not independent. As a result, the independence of these random variables is a heuristic assumption.

2. It is assumed that $T_0 - T_{(2^m q)}$ follows a normal distribution. A sufficient condition for $T_0 - T_{(2^m q)}$ to follow a normal distribution is that T_0 and $T_{(2^m q)}$ are *independent* normal variates. Since the randomness of both T_0 and $T_{(2^m q)}$ arise from the randomness in $P_1, \ldots, P_N$, they are clearly not independent. As a result, the assumption that $T_0 - T_{(2^m q)}$ follows a normal distribution is also a heuristic assumption.

The net effect of the above two assumptions is that the test statistics corresponding to different choices of the sub-key are independent.

3.2 Hypothesis Testing Based Analysis

Statistical hypothesis testing for analysing block cipher cryptanalysis was carried out in [2] in the context of distinguishing attacks. For analysing linear cryptanalysis based key recovery attacks, the hypothesis testing based approach was used in [25] as a method for overcoming some of the theoretical limitations of the order statistics based analysis. Subsequently, hypothesis testing based approach for analysing key recovery attacks in the context of key dependent assumptions was performed in [7].

The idea of the hypothesis testing based approach is simple and intuitive. For each choice κ of the target sub-key, let H_0 be the null hypothesis that κ is correct and H_1 be the alternative hypothesis that κ is incorrect. The test statistic T_κ is used to test H_0 against H_1 where the distributions of T_κ are as in (16) for both $\kappa = \kappa^*$ and $\kappa \neq \kappa^*$. From (16), we get $E[T_{\kappa^*}] = \mu_0$ and $E[T_\kappa] = \nu$. Later on we will see that $\mu_0 = \nu + \delta$, where $\delta > 0$ is a constant. Since $E[T_{\kappa^*}] = \mu_0 > \nu = E[T_\kappa]$, the following hypothesis test is considered.

$$\left.\begin{array}{l} H_0 : \kappa \text{ is correct; versus } H_1 : \kappa \text{ is incorrect.} \\ \text{Decision rule: Reject } H_0 \text{ if } T_\kappa \leq t. \end{array}\right\} \tag{18}$$

Here t is a threshold whose exact value is determined depending on the desired success probability and advantage. The idea of the test is the following. The mean μ_0 under H_0 is greater than the mean ν under H_1, so, if the value of the test statistic is lesser than a certain threshold, it is guessed that H_0 does not hold.

Such a hypothesis test gives rise to two kinds of errors: H_0 is rejected when it holds which is called the Type-1 error; and H_0 is accepted when it does not hold which is called the Type-2 error. If a Type-1 error occurs, then $\kappa = \kappa^*$ is the correct value of the target sub-key but, the test rejects it and so the attack fails to recover the correct value. The attack is successful if and only if Type-1 error does not occur. So, the success probability $P_S = 1 - \Pr[\text{Type-1 error}]$. On the other hand, for every Type-2 error, an incorrect value of κ gets labelled as a candidate key. As a result, the number of times that Type-2 errors occurs is the size of the list of candidate keys.

Theorem 1. *Let $\kappa^* \in \{0,1\}^m$. For $\kappa \in \{0,1\}^m$, let T_κ be 2^m random variables, where $T_{\kappa^*} \sim \mathcal{N}(\mu_0, \sigma_0^2)$, and for $\kappa \neq \kappa^*$, $T_\kappa/\omega \sim \chi^2_\nu$ for some constant $\omega > 0$. Suppose the hypothesis test given in (18) is applied to T_κ for all $\kappa \in \{0,1\}^m$. Let $P_S = 1 - \Pr[\text{Type-1 error}]$ and the expected number of times that Type-2 errors occurs is 2^{m-a}. Then*

$$P_S = \Phi\left(\frac{\mu_0 - \omega\gamma}{\sigma_0}\right) \tag{19}$$

where $\gamma = \Psi^{-1}\left(1 - \frac{2^{m-a-1}}{2^m - 1}\right)$.

Proof. Let $\alpha = \Pr[\text{Type-1 error}]$ and $\beta = \Pr[\text{Type-2 error}]$ and so $P_S = 1-\alpha$. For each $\kappa \neq \kappa^*$, let Z_κ be a binary valued random variable which takes the value 1 if and only if a Type-2 error occurs for κ. So, $\Pr[Z_\kappa = 1] = \beta$. The size of the list of candidate keys returned by the test is $\sum_{\kappa \neq \kappa^*} Z_\kappa$ and so the expected size of the list of candidate keys is

$$E\left[\sum_{\kappa \neq \kappa^*} Z_\kappa\right] = \sum_{\kappa \neq \kappa^*} E\left[Z_\kappa\right] = \sum_{\kappa \neq \kappa^*} \Pr[Z_\kappa = 1] = (2^m - 1)\beta. \tag{20}$$

The expected number of times that Type-2 errors occurs is 2^{m-a}. So,

$$\beta = \frac{2^{m-a}}{2^m - 1}. \tag{21}$$

The Type-1 and Type-2 error probabilities are calculated as follows.

$$\begin{aligned} \alpha &= \Pr[\text{Type-1 error}] \\ &= \Pr[T_\kappa \leq t | H_0 \text{ holds}] \\ &= \Pr[T_{\kappa^*} \leq t] \\ &= \Phi\left(\frac{t-\mu_0}{\sigma_0}\right); \end{aligned} \tag{22}$$

$$\begin{aligned} \beta &= \Pr[\text{Type-2 error}] \\ &= \Pr[T_\kappa > t | H_1 \text{ holds}] = \Pr[T_\kappa/\omega > t/\omega | H_1 \text{ holds}] \\ &= 1 - \Psi_\nu(t/\omega). \end{aligned} \tag{23}$$

Using $\beta = 2^{m-a}/(2^m - 1)$ in (23), we obtain

$$t = \omega \Psi_\nu^{-1}\left(1 - \frac{2^{m-a-1}}{2^m - 1}\right) = \omega\gamma. \tag{24}$$

Substituting t in (22) and noting that $P_S = 1 - \alpha$, we obtain

$$P_S = \Phi\left(\frac{\mu_0 - \omega\gamma}{\sigma_0}\right).$$

□

Remarks:

1. Note that $\gamma = \Psi^{-1}\left(1 - 2^{m-a-1}/(2^m - 1)\right) \geq 0$.
2. The computation in (20) does not require the Z_κ's or the T_κ's to be independent.
3. The theoretical limitations of the order statistics based analysis (namely, m and $m - a$ are large and the heuristic assumption that the T_κ's are independent) are not present in the hypothesis testing based analysis.
4. Comparing (19) to (17), we find that the two expressions are equal under the following three assumptions:
   (a) $2^m/(2^m - 1) \approx 1$: this holds for moderately large values of m, but, is not valid for small values of m.
   (b) $\sigma_0 \gg \sigma_q$: this assumption was used in [28].
   (c) $\omega \approx 1$.

In the rest of the work, we will use (19) as the expression for the success probability.

4 General Key Randomisation Hypotheses

At this point it is important to make the distinction between multiple and multidimensional linear cryptanalysis as it appears in the literature. Multiple linear cryptanalysis [4] refers to linear attacks using ℓ linear approximations where the linear approximations are assumed to be *statistically independent*. Whereas in multidimensional linear cryptanalysis [16] the attacker exploits all linear approximations with linear masks $(\Gamma_P, \Gamma_B) \neq (0,0)$ in a linear space. In other words, in multidimensional linear cryptanalysis the linear approximations are not assumed to be statistically independent. Therefore, in case of multidimensional linear cryptanalysis the attacker works with the joint distribution of the ℓ linear approximations whereas in case of multiple linear cryptanalysis the attacker works with the marginal distributions.

Recall the definitions of $q_{\kappa,\kappa^*}(\eta)$ and $p_{\kappa^*}(\eta)$ from (5). The corresponding biases are $\epsilon_{\kappa,\kappa^*}(\eta)$ and $\epsilon_{\kappa^*}(\eta)$. For obtaining the distributions of T_{κ^*} and T_κ, $\kappa \neq \kappa^*$, it is required to hypothesise the behaviour of $p_{\kappa^*}(\eta)$ and $q_{\kappa,\kappa^*}(\eta)$, respectively.

4.1 General Multidimensional Key Randomisation Hypotheses

The two standard multidimensional key randomisation hypotheses are the following.

> **Standard multidimensional right key randomisation hypothesis:** For every choice of κ^*, $p_{\kappa^*}(\eta) = p_\eta$, such that $0 < p_\eta < 1$ and $\sum_{\eta \in \{0,1\}^\ell} p_\eta = 1$.
> **Standard multidimensional wrong key randomisation hypothesis:** For every choice of κ^* and $\kappa \neq \kappa^*$, $q_{\kappa,\kappa^*}(\eta) = 2^{-\ell}$ for all $\eta \in \{0,1\}^\ell$.

The standard wrong key randomisation hypothesis for $\ell = 1$ was formally considered in [15] and later generalised to $\ell > 1$ in [16]. Based on the work in [14] the standard wrong key randomisation for $\ell = 1$ was modified in [11] and for $\ell > 1$ in [7]. An earlier version [6] of [7] uses the following formulation.

> **Adjusted multidimensional wrong key randomisation hypothesis:** For each $\kappa \neq \kappa^*$, $\eta \in \{0,1\}^\ell$, $q_{\kappa,\kappa^*}(\eta) \sim \mathcal{N}\left(\frac{1}{2^\ell}, \frac{1}{2^{n+\ell}}\left(1 - \frac{1}{2^\ell}\right)\right)$ and $q_{\kappa,\kappa^*}(0), \ldots, q_{\kappa,\kappa^*}(2^\ell - 1)$ are independent.

Remarks:

1. In this hypothesis, there is no explicit dependence of the bias on either κ or κ^*.
2. As $q_{\kappa,\kappa^*}(\eta)$ is a probability, $0 \leq q_{\kappa,\kappa^*}(\eta) \leq 1$. On the other hand, a random variable following a normal distribution can take any real value. So, the above hypothesis may lead to $q_{\kappa,\kappa^*}(\eta)$ taking a value outside the range $[0,1]$ which is not meaningful. As a result, the adjusted wrong key randomisation hypothesis must necessarily be considered to be a *heuristic* assumption.
3. The probability that $q_{\kappa,\kappa^*}(\eta)$ takes values outside of $[0,1]$ can be bounded as follows.

$$
\begin{aligned}
&\Pr[q_{\kappa,\kappa^*}(\eta) < 0 \text{ or } q_{\kappa,\kappa^*}(\eta) > 1] \\
&= \Pr[q_{\kappa,\kappa^*}(\eta) < 0] + \Pr[q_{\kappa,\kappa^*}(\eta) > 1] \\
&= \Pr[q_{\kappa,\kappa^*}(\eta) - 2^{-\ell} < -2^{-\ell}] + \Pr[q_{\kappa,\kappa^*}(\eta) - 2^{-\ell} > 1 - 2^{-\ell}] \\
&\leq \Pr[|q_{\kappa,\kappa^*}(\eta) - 2^{-\ell}| < 2^{-\ell}] + \Pr[|q_{\kappa,\kappa^*}(\eta) - 2^{-\ell}| > 1 - 2^{-\ell}] \\
&\leq \frac{1}{2^{n+\ell}}\left(1 - \frac{1}{2^\ell}\right) \times \frac{1}{2^{-2\ell}} + \frac{1}{2^{n+\ell}}\left(1 - \frac{1}{2^\ell}\right) \times \frac{1}{(1 - 2^{-\ell})^2} \quad \text{[By Chebyshev's inequality]} \\
&= \frac{2^\ell - 1}{2^n} + \frac{1}{2^n(2^\ell - 1)} \leq 2^{-(n-\ell)} + \frac{1}{2^n(2^\ell - 1)} \\
&\approx 2^{-(n-\ell)} + 2^{-(n+\ell)}.
\end{aligned}
$$

In other words, $q_{\kappa,\kappa^*}(\eta)$ takes values outside $[0,1]$ with exponentially low probability, provided that $n-\ell$ is large; if $n-\ell$ is not too large, then the probability is not negligible.

Modification of the right key randomisation hypothesis was first considered in [17] in the context of multidimensional linear cryptanalysis. In [17], Theorem 22 of [13] was taken as the right key hypotheses, i.e., it was assumed that even for the right choice of the target sub-key, the probability of a linear approximation follows a normal distribution. This assumption was later used in [7] and the following can be stated.

Adjusted multidimensional right key randomisation hypothesis: For all $\eta \in \{0,1\}^\ell$, $p_{\kappa^*}(\eta) \sim \mathcal{N}\left(p_\eta, \sigma^2\right)$, where $0 < p_\eta < 1$ is a constant such that $\sum_{\eta\in\{0,1\}^\ell} p_\eta = 1$ and each subset of $2^\ell - 1$ random variables out of 2^ℓ possible random variables $q_{\kappa,\kappa^*}(\eta)$ are independent and this set determines the remaining random variable uniquely.

Remarks:

1. The first two remarks for adjusted multidimensional wrong key randomisation hypothesis also holds for adjusted multidimensional right key randomisation hypothesis.
2. Since the form of σ^2 is not given nothing can be said about the probability that $p_{\kappa^*}(\eta)$ lies outside $[0,1]$.
3. The random variables $p_{\kappa^*}(0), \ldots, p_{\kappa^*}(2^\ell - 1)$ are not assumed to be independent. On the other hand, while the marginals are assumed to follow normal distribution, no assumption is made on the joint distribution. The normality of the marginals do not imply that the joint distribution is also normal.
4. The assumption that each possible subset of $2^\ell - 1$ random variables out of 2^ℓ possible random variables $p_{\kappa^*}(\eta)$ are independent is a heuristic assumption. The rationale for this assumption is perhaps to justify that the distribution of the test statistic under the right key follows a non-central chi-squared distribution. This assumption, however, is not sufficient for this purpose, as we discuss later.

Let C be the expected value of $2^\ell \sum_{\eta\in\{0,1\}^\ell}(p_{\kappa^*}(\eta) - 2^{-\ell})^2$, i.e.,

$$C = 2^\ell \sum_{\eta\in\{0,1\}^\ell} E[(p_{\kappa^*}(\eta) - 2^{-\ell})^2]. \tag{25}$$

In [7], the value of σ^2 in the adjusted right key randomisation hypothesis is expressed in terms of C and the capacity $C^{(\mathrm{md})}$ in the following manner.

$$\begin{aligned} C &= 2^\ell \sum_{\eta\in\{0,1\}^\ell} E[(p_{\kappa^*}(\eta) - 2^{-\ell})^2] \\ &= 2^\ell \sum_{\eta\in\{0,1\}^\ell} E[(p_{\kappa^*}(\eta) - p_\eta)^2 + (p_\eta - 2^{-\ell})^2 + 2(p_\eta - 2^{-\ell})(p_{\kappa^*}(\eta) - p_\eta)] \\ &= 2^{2\ell}\sigma^2 + C^{(\mathrm{md})} \\ \Rightarrow \sigma^2 &= \frac{C - C^{(\mathrm{md})}}{2^{2\ell}}. \end{aligned} \tag{26}$$

Motivated by the description of the standard and adjusted right and wrong key randomisation hypotheses in [7] we formulate the following general multidimensional key randomisation hypotheses for both the right and the wrong key.

General multidimensional right key randomisation hypothesis: For all $\eta \in \{0,1\}^\ell$, $p_{\kappa^*}(\eta) \sim \mathcal{N}\left(p_\eta, s_0^2\right)$, where $0 < p_\eta < 1$ is a constant such that $\sum_{\eta\in\{0,1\}^\ell} p_\eta = 1$ and each subset of $2^\ell - 1$ random variables out of 2^ℓ possible random variables $p_{\kappa^*}(\eta)$ are independent and this set determines the remaining random variable uniquely. Further, $s_0^2 \leq 2^{-n}$.
General multidimensional wrong key randomisation hypothesis: For each $\kappa \neq \kappa^*$, $\eta \in \{0,1\}^\ell$, $q_{\kappa,\kappa^*}(\eta) \sim \mathcal{N}\left(\frac{1}{2^\ell}, s_1^2\right)$, where $s_1^2 \leq 2^{-n}$; and $q_{\kappa,\kappa^*}(0), \ldots, q_{\kappa,\kappa^*}(2^\ell - 1)$ are independent.

The heuristic nature of the adjusted right and wrong key hypotheses discussed earlier also hold for the general hypotheses.

1. As $s_1 \downarrow 0$, the random variable $q_{\kappa,\kappa^*}(\eta)$ becomes degenerate and takes the value $2^{-\ell}$. In this case, the general multidimensional wrong key randomisation hypothesis becomes the standard multidimensional wrong key randomisation hypotheses.

2. For $s_1^2 = \frac{1}{2^{n+\ell}}\left(1 - \frac{1}{2^\ell}\right)$, the general multidimensional wrong key randomisation hypothesis becomes the adjusted multidimensional wrong key randomisation hypothesis.

3. As $s_0 \downarrow 0$, the general multidimensional right key randomisation hypothesis reduces to the standard multidimensional right key randomisation hypothesis.

4. For $s_0^2 = \sigma^2$, the general multidimensional right key randomisation hypothesis becomes the adjusted multidimensional right key randomisation hypothesis.

4.2 General Multiple Key Randomisation Hypotheses

For a single linear approximation, the standard/adjusted/general wrong and right key randomisation hypotheses have been proposed in the literature [15, 11, 27]. The extension to multiple linear cryptanalysis is essentially extending to several independent linear approximations. This requires making assumptions on $p_{\kappa^*,i}$ and $q_{\kappa,\kappa^*,i}$ given by (6).

The standard multiple right and wrong key randomisation hypotheses were first considered in [4] and can be stated as follows.

Standard multiple right key randomisation hypothesis: For each choice of κ^* and for $i = 1, \ldots, \ell$, $p_{\kappa^*,i} = p_i$ with $0 < p_i < 1$.
Standard multiple wrong key randomisation hypothesis: For each choice of κ^* and $\kappa \neq \kappa^*$, and for $i = 1, \ldots, \ell$, $q_{\kappa,\kappa^*,i} = 1/2$.

Based on [14], the multiple wrong key randomisation hypothesis was modified in [6] (which is an earlier version of [7]) in the following manner.

Adjusted multiple wrong key randomisation hypothesis: For each $\kappa \neq \kappa^*$ and for $i = 1, \ldots, \ell$, $q_{\kappa,\kappa^*,i} \overset{\text{i.i.d.}}{\sim} \mathcal{N}\left(\frac{1}{2}, 2^{-n-2}\right)$.

Remarks: The remarks given below are essentially extensions of similar comments given in [27] in the context of single linear approximation.

1. There is no explicit dependence of the bias on either κ or κ^*.

2. As $q_{\kappa,\kappa^*,i}$ is a probability it takes values from $[0, 1]$. On the other hand, a random variable following a normal distribution can take any real value. So, similar to the multidimensional case, here also, the above hypothesis may lead to $q_{\kappa,\kappa^*,i}$ taking a value outside the range $[0, 1]$ which is not meaningful. Hence, the adjusted wrong key randomisation hypothesis must necessarily be considered to be a *heuristic* assumption.

3. The variance 2^{-n} is an exponentially decreasing function of n and by Chebyshev's inequality $\Pr[|q_{\kappa,\kappa^*,i} - 1/2| > 1/2] \leq 4 \cdot 2^{-n-2} = 2^{-n}$. In other words, $q_{\kappa,\kappa^*,i}$ takes values outside $[0,1]$ with exponentially low probability.

Modification of the standard right key randomisation hypothesis in the context of multiple linear approximation was considered in [7]. The formulation given below follows [6].

> **Adjusted multiple right key randomisation hypothesis:** For all κ^* and for $i = 1, \ldots, \ell$, $p_{\kappa^*,i} \overset{\text{i.i.d.}}{\sim} \mathcal{N}\left(p_i, \sigma^2\right)$.

Remarks: The first two remarks for the adjusted multiple wrong key randomisation hypothesis also hold in this case. As the mathematical form of σ^2 is not given, nothing can be said about the probability that a particular $p_{\kappa^*,i}$ lies outside $[0,1]$.

Motivated by the description of the standard and adjusted right and wrong key randomisation hypotheses in [7] we formulate the following general multiple key randomisation hypotheses for both the right and the wrong key.

> **General multiple right key randomisation hypothesis:** For all κ^* and for $i = 1, \ldots, \ell$; $p_{\kappa^*,i} \overset{\text{i.i.d.}}{\sim} \mathcal{N}\left(p_i, s_0^2\right)$, where $p_i \in [0,1]$ and $s_0^2 \leq 2^{-n}$.
> **General multiple wrong key randomisation hypothesis:** For all κ^* and $\kappa \neq \kappa^*$, and for $i = 1, \ldots, \ell$; $q_{\kappa,\kappa^*,i} \overset{\text{i.i.d.}}{\sim} \mathcal{N}\left(\frac{1}{2}, s_1^2\right)$, where $s_1^2 \leq 2^{-n}$.

The heuristic nature of the adjusted right and wrong key hypotheses discussed earlier also hold for the general hypotheses. We note the following.

1. As $s_0 \downarrow 0$, the random variable $p_{\kappa^*,i}$ becomes degenerate and takes the value of the constant p_i. In this case, the general multiple right key randomisation hypothesis becomes the standard multiple right key randomisation hypothesis.

2. For $s_0^2 = \sigma^2$, the general multiple right key randomisation hypothesis becomes the adjusted multiple right key randomisation hypothesis.

3. As $s_1 \downarrow 0$, the random variable $q_{\kappa,\kappa^*,i}$ becomes degenerate and takes the value $1/2$. In this case, the general multiple wrong key randomisation hypothesis becomes the standard multiple wrong key randomisation hypothesis.

4. For $s_1^2 = 2^{-n-2}$, the general multiple wrong key randomisation hypothesis becomes the adjusted multiple wrong key randomisation hypothesis.

4.3 Differences with the Formulation of the Various Hypotheses in [7]

We have postulated the various hypotheses as conditions on p_{κ^*} and q_{κ,κ^*} given by (5) in the case of multidimensional linear cryptanalysis and as conditions on $p_{\kappa^*,i}$ and $q_{\kappa,\kappa^*,i}$ given by (6) in the case of multiple linear cryptanalysis. This follows the approach taken in an earlier version [6] of [7]. The hypotheses in the published version [7] are of the following types.

1. For the multidimensional case, the adjusted right key randomisation hypothesis is formulated as an assumption on p_{κ^*} as in the earlier version [6] while the adjusted wrong key randomisation hypothesis is formulated as an assumption on $Q_{\kappa,\eta} - N2^{-\ell}$.

2. For the multiple case, the adjusted right key randomisation hypothesis is formulated as an assumption on $Y_{\kappa^*,i} - N/2$ while the adjusted wrong key randomisation hypothesis is formulated as an assumption on $Y_{\kappa,i} - N/2$.

So, in [7], out of four cases, in one case the assumption is on underlying probability while in the other three cases, the assumptions are on derived random variables. In our opinion, if one follows the work in [14], then the assumptions should be on the underlying probabilities rather than on the derived random variables. That is why we have chosen to state the hypotheses as formulated in [6].

We emphasise that the general formulation that we present here and the detailed consideration of the heuristic nature of these hypotheses do not appear either in [6] or in [7].

5 Heuristic Distributions of the Test Statistics

The form of the test statistic T_κ is given by (12) for multidimensional linear cryptanalysis and by (13) for multiple linear cryptanalysis. As outlined in Section 3, to obtain the success probability it is required to obtain the distributions of T_κ for both the right and wrong choices of κ. In the case of mutidimensional linear cryptanalysis, T_κ is defined from the $Q_{\kappa,\eta}$'s and so to obtain the distribution of T_κ it is required to obtain the distribution of $Q_\kappa = (Q_{\kappa,0}, \ldots, Q_{\kappa,2^\ell-1})$. Similarly, in the case of multiple linear cryptanalysis, T_κ is defined from $Y_{\kappa,i}$ and to obtain the distribution of T_κ it is required to obtain the distribution of $(Y_{\kappa,1}, \ldots, Y_{\kappa,\ell})$.

The derivations of the distributions of T_κ under the various settings are heuristic and provide only a rough approximation where it is hard to estimate the error in approximation. We explain this issue in the context of multidimensional linear cryptanalysis where sampling with replacement is used, but, similar considerations hold in the other settings.

In the setting of multidimensional linear cryptanalysis, T_κ given by (12) is defined from the random vector $Q_\kappa = (Q_{\kappa,0}, \ldots, Q_{\kappa,2^\ell-1})$ where $Q_{\kappa,\eta}$'s are defined as in (9) satisfying the condition given in (10). For sampling with replacement, Q_κ follows a multinomial distribution and $Q_{\kappa,\eta}$ follows $\mathsf{Bin}(N, p_\kappa(\eta))$ where $p_\kappa(\eta)$ is heuristically assumed to follow a normal distribution. The $p_\kappa(\eta)$'s are not assumed to be independent.

The mean vector of the random vector Q_κ is $(Np_\kappa(0), \ldots, Np_\kappa(2^\ell-1))$. The distribution of a random variable whose parameters are also random variables is called a compound distribution. If the $p_\kappa(\eta)$'s took values in $[0,1]$, then it would have been possible to formally consider the distribution of Q_κ. Since the $p_\kappa(\eta)$'s are assumed to follow normal, they can take values outside of $[0,1]$ and so, we see no way of formally deriving the distribution of Q_κ. The heuristic assumption of normality on $p_\kappa(\eta)$ implies that the distribution of Q_κ and hence of T_κ are both fundamentally heuristic assumptions. It is not possible to derive these distributions formally; one can only try to provide some justification for the heuristic assumptions.

The key randomisation hypotheses postulates that the marginals $p_\kappa(\eta)$'s are approximately normal. It does not postulate anything about the joint distribution of the $p_\kappa(\eta)$'s. If the marginals are normal, it does not necessarily follow (in fact, it mostly does not) that the joint distribution is also normal. From the normal assumption on the marginals $p_\kappa(\eta)$'s, we can only heuristically argue (as argued in Section 5.1 below) that each of the marginals $Q_{\kappa,\eta}$ follow an approximate normal distribution. Nothing can be proved about the joint distribution of the $Q_{\kappa,\eta}$'s. Instead, it is required to make a heuristic assumption that Q_κ follows a multivariate normal distribution. Further, this heuristic assumption does not clarify the nature of the variance-covariance matrix of the multivariate normal distribution of Q_κ.

The form of T_κ given by (12) suggests that the distribution of T_κ should be given by a suitable chi-squared distribution. This would follow if it is possible to show that the Q_κ approximately follows a multivariate normal distribution whose variance-covariance matrix satisfies the conditions of Theorem A.1 of Appendix 6. Since this cannot be proved formally, it is heuristically assumed that Q_κ follows an appropriate multivariate normal so that the distribution of T_κ can be approximated by a chi-squared distribution.

Note that for the actual computation of the parameters (degrees of freedom and the non-centrality parameter) of the chi-squared distribution, it is sufficient to have the mean vector for Q_κ. Since it is possible to heuristically justify that the marginals for Q_κ follow an approximate normal distribution, an approximation of the mean vector for Q_κ can be obtained. So, it is possible to obtain approximate values of the parameters of the chi-squared

distribution which T_κ is heuristically assumed to follow.

This issues of heuristic derivation of the distribution of T_κ is not particular to the use of the general key randomisation hypotheses. It is also relevant in the context of adjusted key randomisation hypotheses as considered in [7]. The work [7] does not provide an explicit deduction of the distribution of T_κ. If the derivation had been considered in details in [7], then the issues discussed above would have appeared.

5.1 Multidimensional Case

The distributions of T_{κ^*} and T_κ depend on whether $P_1, \ldots, P_N$ are chosen with or without replacement. We separately consider both these cases. As mentioned above, the distributions of T_{κ^*} and T_κ require the distribution of Q_κ and the discussion below provides a heuristic justification that the marginals $Q_{\kappa,\eta}$ follow an approximate normal distribution. The analysis is similar to the analysis for the case of single linear approximation given in [27]. Before proceeding, we state some approximations that will be required later.

In the general multidimensional key randomisation hypotheses, we have $s_0^2, s_1^2 \leq 2^{-n}$. Let $\theta_0^2 = s_0^2 2^{n/2} \leq 2^{-n/2}$. By Chebyshev's inequality, we have for all $\eta \in \{0,1\}^\ell$

$$\Pr[|p_{\kappa^*}(\eta) - p_\eta| > \theta_0] \leq \frac{Var(p_{\kappa^*}(\eta))}{\theta_0^2} = s_0^2/\theta_0^2 \leq 2^{-n/2}. \tag{27}$$

So, with exponentially low probability, $p_{\kappa^*}(\eta)$ takes values outside the range $[p_\eta - \theta_0, p_\eta + \theta_0]$. For $\mathfrak{p}_\eta \in [p_\eta - \theta_0, p_\eta + \theta_0]$ and $\theta_\eta = \mathfrak{p}_\eta - 2^{-\ell}$, we have $\epsilon_\eta - \theta_0 \leq \theta_\eta \leq \epsilon_\eta + \theta_0$, where $\epsilon_\eta = p_\eta - 2^{-\ell}$. So

$$\begin{aligned}
\mathfrak{p}_\eta(1-\mathfrak{p}_\eta) &= (2^{-\ell} + \theta_\eta)(1 - 2^{-\ell} - \theta_\eta) \\
&= 2^{-\ell}(1-2^{-\ell}) + \theta_\eta\left(1 - 2^{-\ell+1}\right) - \theta_\eta^2 \\
&\geq 2^{-\ell}(1-2^{-\ell}) + (\epsilon_\eta - \theta_0)\left(1 - 2^{-\ell+1}\right) - (\epsilon_\eta + \theta_0)^2 \\
&\approx 2^{-\ell}(1-2^{-\ell}) + (\epsilon_\eta - \theta_0)\left(1 - 2^{-\ell+1}\right) \\
&\geq 2^{-\ell}(1-2^{-\ell}) + (\epsilon_\eta - 2^{-n/4})\left(1 - 2^{-\ell+1}\right) \\
&\approx 2^{-\ell}(1-2^{-\ell}) + \epsilon_\eta\left(1 - 2^{-\ell+1}\right).
\end{aligned} \tag{28}$$

under the assumption that $(\epsilon_\eta + \theta_0)^2$ and $2^{-n/4}$ are negligible. Proceeding with the approximation $\mathfrak{p}_\eta(1-\mathfrak{p}_\eta) \approx 2^{-\ell}(1-2^{-\ell}) + \epsilon_\eta\left(1-2^{-\ell+1}\right)$ it does not seem possible to obtain a known tractable form of the distribution of T_{κ^*}. Perhaps to avoid this problem, [7] replaces $\mathfrak{p}_\eta(1-\mathfrak{p}_\eta)$ by $2^{-\ell}$. This is clearly a heuristic assumption made to make sure that the distribution is tractable. We will also proceed with a similar heuristic assumption. Instead of assuming $\mathfrak{p}_\eta(1-\mathfrak{p}_\eta) \approx 2^{-\ell}$, we will assume

$$\mathfrak{p}_\eta(1-\mathfrak{p}_\eta) \approx 2^{-\ell}(1-2^{-\ell}). \tag{29}$$

for $\mathfrak{p}_\eta \in [p_\eta - \theta_0, p_\eta + \theta_0]$.

Let $\vartheta_1^2 = s_1^2 2^{n/2} \leq 2^{-n/2}$ and as above, we have by Chebyshev's inequality

$$\Pr[|q_{\kappa,\kappa^*}(\eta) - 2^{-\ell}| > \vartheta_1] \leq s_1^2/\vartheta_1^2 = 2^{-n/2}. \tag{30}$$

Further, let $\vartheta = \mathfrak{q}_\eta - 2^{-\ell}$ so that for $\mathfrak{q}_\eta \in [2^{-\ell} - \vartheta_1, 2^{-\ell} + \vartheta_1]$,

$$\begin{aligned}
\mathfrak{q}_\eta(1-\mathfrak{q}_\eta) &\geq 2^{-\ell}(1-2^{-\ell}) - 2^{-n/4}\left(1 - 2^{-\ell+1}\right) - 2^{-n/2} \\
&\approx 2^{-\ell}(1-2^{-\ell}).
\end{aligned} \tag{31}$$

under the assumption that $2^{-n/4}$ is negligible.

Remark: Note that for small values of n ignoring $2^{-n/4}$ is not justified. In that case, for $\kappa \neq \kappa^*$ we may approximate $\mathfrak{q}_\eta(1-\mathfrak{q}_\eta)$ by $2^{-\ell}(1-2^{-\ell}) - 2^{-n/4}\left(1-2^{-\ell+1}\right)$, i.e., we ignore $2^{-n/2}$.

5.1.1 Distributions of T_{κ^*} and $T_\kappa, \kappa \neq \kappa^*$ under Uniform Random Sampling with Replacement

In this case, $P_1, \ldots, P_N$ are chosen under uniform random sampling with replacement so that $P_1, \ldots, P_N$ are assumed to be independent and uniformly distributed over $\{0,1\}^n$.

First consider T_{κ^*} whose distribution is determined from the distribution of $p_{\kappa^*}(\eta)$'s. Recall that $Q_{\kappa^*,\eta} = \#\{j \in \{1,2,\ldots,N\} : X_{\kappa,j} = \eta\} = W_{\kappa^*,1} + \cdots + W_{\kappa^*,N}$, where

$$W_{\kappa^*,j} = \begin{cases} 1 & \text{if } X_{\kappa,j} = \eta \\ 0 & \text{if } X_{\kappa,j} \neq \eta. \end{cases}$$

Thus, each $W_{\kappa,j}$ is a Bernoulli distributed random variable with probability of success $p_{\kappa^*}(\eta)$. Since $P_1, \ldots, P_N$ are independent, the random variables $W_{\kappa^*,1}, \ldots, W_{\kappa^*,N}$ are also independent. Hence, $Q_{\kappa^*,\eta}$ is a Binomial$(N, p_{\kappa^*}(\eta))$ variate. Under the general multidimensional right key randomisation assumption, $p_{\kappa^*}(\eta)$ is modelled as a random variable following $\mathcal{N}(p_\eta, s_0^2)$ and so the density function of $p_{\kappa^*}(\eta)$ is $\mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2)$. The distribution function of $Q_{\kappa^*,\eta}$ is approximated as follows:

$$\begin{aligned} \Pr[Q_{\kappa^*,\eta} \leq x] &= \sum_{\mathfrak{k} \leq x} \Pr[Q_{\kappa^*,\eta} = \mathfrak{k}] \\ &\approx \sum_{\mathfrak{k} \leq x} \int_{-\infty}^{\infty} \binom{N}{\mathfrak{k}} \mathfrak{p}_\eta^{\mathfrak{k}} (1-\mathfrak{p}_\eta)^{N-\mathfrak{k}} \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2) d\mathfrak{p}_\eta \\ &= \int_{-\infty}^{\infty} \left(\sum_{\mathfrak{k} \leq x} \binom{N}{\mathfrak{k}} \mathfrak{p}_\eta^{\mathfrak{k}} (1-\mathfrak{p}_\eta)^{N-\mathfrak{k}} \right) \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2) d\mathfrak{p}_\eta. \end{aligned} \tag{32}$$

The sum within the integral is the distribution function of the binomial distribution and can be approximated by $\mathcal{N}(N\mathfrak{p}_\eta, N\mathfrak{p}_\eta(1-\mathfrak{p}_\eta))$. In this approximation, the variance of the normal also depends on $\mathfrak{p}_\eta$ which makes it difficult to proceed with further analysis. Using (29), we approximate $\mathfrak{p}_\eta(1-\mathfrak{p}_\eta))$ by $2^{-\ell}(1-2^{-\ell})$. As mentioned earlier this is a heuristic assumption made to get a tractable form of the distribution of T_{κ^*}. So, we break up the integral in (32) in a manner such that the approximation $\mathfrak{p}_\eta(1-\mathfrak{p}_\eta) \approx 2^{-\ell}(1-2^{-\ell})$ can be made in the range

$p_\eta - \theta_0$ to $p_\eta + \theta_0$ and it is possible to show that the contribution to (32) for $\mathfrak{p}_\eta$ outside this range is negligible.

$$
\begin{aligned}
&\Pr[Q_{\kappa^*,\eta} \le x] \\
&= \int_{p_\eta-\theta_0}^{p_\eta+\theta_0} \left(\sum_{\mathfrak{k}\le x} \binom{N}{\mathfrak{k}} \mathfrak{p}_\eta^{\mathfrak{k}} (1-\mathfrak{p})^{N-\mathfrak{k}} \right) \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2) d\mathfrak{p}_\eta \\
&\quad + \int_{-\infty}^{p_\eta-\theta_0} \left(\sum_{\mathfrak{k}\le x} \binom{N}{\mathfrak{k}} \mathfrak{p}_\eta^{\mathfrak{k}} (1-\mathfrak{p}_\eta)^{N-\mathfrak{k}} \right) \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2) d\mathfrak{p}_\eta + \\
&\quad \int_{p_\eta+\theta_0}^{\infty} \left(\sum_{\mathfrak{k}\le x} \binom{N}{\mathfrak{k}} \mathfrak{p}_\eta^{\mathfrak{k}} (1-\mathfrak{p}_\eta)^{N-\mathfrak{k}} \right) \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2) d\mathfrak{p}_\eta \qquad (33) \\
&\le \int_{p_\eta-\theta_0}^{p_\eta+\theta_0} \left(\sum_{\mathfrak{k}\le x} \binom{N}{\mathfrak{k}} \mathfrak{p}_\eta^{\mathfrak{k}} (1-\mathfrak{p}_\eta)^{N-\mathfrak{k}} \right) \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2) d\mathfrak{p}_\eta + \int_{-\infty}^{p_\eta-\theta_0} \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2) d\mathfrak{p}_\eta + \int_{p_\eta+\theta_0}^{\infty} \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2) d\mathfrak{p}_\eta \\
&= \int_{p_\eta-\theta_0}^{p_\eta+\theta_0} \left(\sum_{\mathfrak{k}\le x} \binom{N}{\mathfrak{k}} \mathfrak{p}_\eta^{\mathfrak{k}} (1-\mathfrak{p}_\eta)^{N-\mathfrak{k}} \right) \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2) d\mathfrak{p}_\eta + \Pr[|p_{\kappa^*}(\eta) - p_\eta| > \theta_0] \\
&\le \int_{p_\eta-\theta_0}^{p_\eta+\theta_0} \left(\sum_{\mathfrak{k}\le x} \binom{N}{\mathfrak{k}} \mathfrak{p}_\eta^{\mathfrak{k}} (1-\mathfrak{p}_\eta)^{N-\mathfrak{k}} \right) \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2) d\mathfrak{p}_\eta + 2^{-n/2} \quad \text{(from (27))} \\
&\approx \int_{p_\eta-\theta_0}^{p_\eta+\theta_0} \left(\sum_{\mathfrak{k}\le x} \binom{N}{\mathfrak{k}} \mathfrak{p}_\eta^{\mathfrak{k}} (1-\mathfrak{p}_\eta)^{N-\mathfrak{k}} \right) \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2) d\mathfrak{p}_\eta. \qquad (34)
\end{aligned}
$$

The sum inside the integral is approximated by the distribution function of $\mathcal{N}(N\mathfrak{p}_\eta, N\mathfrak{p}_\eta(1-\mathfrak{p}_\eta))$. The range of the integration over $\mathfrak{p}_\eta$ is from $p_\eta - \theta_0$ to $p_\eta + \theta_0$. Using (29), it follows that for $\mathfrak{p}_\eta \in [p_\eta - \theta_0, p_\eta + \theta_0]$ the normal distribution $\mathcal{N}(N\mathfrak{p}_\eta, N\mathfrak{p}_\eta(1-\mathfrak{p}_\eta))$ can be approximated as $\mathcal{N}\left(N\mathfrak{p}_\eta, N2^{-\ell}(1-2^{-\ell})\right)$ (i.e., $\mathfrak{p}_\eta(1-\mathfrak{p}_\eta) \approx 2^{-\ell}(1-2^{-\ell})$). Note that the above analysis has been done to ensure that the range of $\mathfrak{p}_\eta$ is such that this approximation is meaningful. Then,

$$
\begin{aligned}
\Pr[Q_{\kappa^*,\eta} \le x] &\approx \int_{p_\eta-\theta_0}^{p_\eta+\theta_0} \left(\int_{-\infty}^{x} \mathfrak{f}\left(x; N\mathfrak{p}_\eta, N2^{-\ell}(1-2^{-\ell})\right) dx \right) \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2) d\mathfrak{p}_\eta. \\
&\le \int_{-\infty}^{\infty} \left(\int_{-\infty}^{x} \mathfrak{f}\left(x; N\mathfrak{p}_\eta, N2^{-\ell}(1-2^{-\ell})\right) dx \right) \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2) d\mathfrak{p}_\eta. \qquad (35) \\
&= \int_{-\infty}^{x} \int_{-\infty}^{\infty} \left(\mathfrak{f}\left(x; N\mathfrak{p}_\eta, N2^{-\ell}(1-2^{-\ell})\right) \mathfrak{f}(\mathfrak{p}; p_\eta, s_0^2) d\mathfrak{p} \right) dx \\
&= \int_{-\infty}^{x} \mathfrak{f}\left(x; Np_\eta, s_0^2 N^2 + N2^{-\ell}(1-2^{-\ell})\right) dx. \qquad (36)
\end{aligned}
$$

The last equality follows from compound normal distribution. For a proof, we refer to the appendix of [27].

From (36), the distribution of $Q_{\kappa^*,\eta}$ is approximately $\mathcal{N}\left(Np_\eta, s_0^2 N^2 + N2^{-\ell}(1-2^{-\ell})\right)$. Consequently, the distribution of $Z_{\kappa^*,\eta} = Q_{\kappa^*,\eta}/N - 2^{-\ell}$ is approximately given as follows:

$$
Z_{\kappa^*,\eta} \sim \mathcal{N}\left(\epsilon_\eta, s_0^2 + \frac{2^{-\ell}(1-2^{-\ell})}{N}\right). \qquad (37)
$$

We have

$$\begin{aligned} T_{\kappa^*} &= N2^\ell \sum_{\eta\in\{0,1\}^\ell} Z^2_{\kappa^*,\eta} \\ &= N\left(2^\ell s_0^2 + \frac{(1-2^{-\ell})}{N}\right) \sum_{\eta\in\{0,1\}^\ell} \frac{Z^2_{\kappa^*,\eta}}{s_0^2 + \frac{2^{-\ell}(1-2^{-\ell})}{N}}. \end{aligned}$$

Theorem 6 of Appendix A.1 lists certain conditions under which T_{κ^*} follows a non-central chi-square distribution with $2^\ell - 1$ degrees of freedom. To apply this result, we assume that $(Z_{\kappa^*,0}, \ldots, Z_{\kappa^*,2^\ell-1})$ follows a multivariate normal distribution $\mathcal{N}(\mu, \Sigma)$ and there exists an $\iota = (\iota_0, \ldots, \iota_{2^\ell-1})$ such that $\iota\Sigma = 0 \Rightarrow \iota\mu^t = 0$; $\Sigma^2 = \Sigma$ with trace of Σ equal to $2^\ell - 1$. Then by Theorem 6 the following approximately holds.

$$\frac{T_{\kappa^*}}{N\left(2^\ell s_0^2 + \frac{1}{N}\left(1-2^{-\ell}\right)\right)} \sim \chi^2_{2^\ell-1}(\delta), \tag{38}$$

where

$$\begin{aligned} \delta &= \sum_{\eta\in\{0,1\}^\ell} \frac{\epsilon_\eta^2}{s_0^2 + \frac{1}{N}(2^{-\ell}(1-2^{-\ell}))} = N2^\ell \sum_{\eta\in\{0,1\}^\ell} \frac{\epsilon_\eta^2}{N2^\ell s_0^2 + (1-2^{-\ell})} \\ &= \frac{NC^{(\mathrm{md})}}{N2^\ell s_0^2 + (1-2^{-\ell})}. \end{aligned} \tag{39}$$

As mentioned earlier, the above assumption is not particular to the case of general key randomisation hypotheses. Though not explicitly stated, such an assumption is also required to justify the distribution of the test statistic in the proof of Theorem 8 in [7].

Consider the case of T_κ, $\kappa \neq \kappa^*$. This requires the distribution of $Q_\kappa = (Q_{\kappa,0}, \ldots, Q_{\kappa,2^\ell-1})$, $\kappa \neq \kappa^*$ and is based on the general wrong key randomisation hypothesis in the multidimensional setting. Under this hypothesis, the $q_{\kappa,\kappa^*}(\eta)$'s are considered to be independent. The distribution of the marginal $Q_{\kappa,\eta}$ (and of $Z_{\kappa,\eta}$) from the distribution of $q_{\kappa,\kappa^*}(\eta)$ is heuristically derived as in the case of $Q_{\kappa^*,\eta}$. The independence of the $q_{\kappa,\kappa^*}(\eta)$ does not, however, imply that the $Q_{\kappa,\eta}$'s are independent. The condition $\sum_{\eta\in\{0,1\}^\ell} Q_{\kappa,\eta} = N$ still hold. So, as in the case of Q_{κ^*}, the heuristic assumptions on the normality of the random vector Q_κ and its variance-covariance matrix are still required. Under such assumptions it is possible to heuristically argue that the following approximately holds.

$$\frac{T_\kappa}{s_1^2 + \frac{1}{N}\left(2^{-\ell}\left(1-2^{-\ell}\right)\right)} = \sum_{\eta\in\{0,1\}^\ell} \frac{Z^2_{\kappa,\eta}}{s_1^2 + \frac{1}{N}\left(2^{-\ell}\left(1-2^{-\ell}\right)\right)} \sim \chi^2_{2^\ell-1}, \quad \kappa \neq \kappa^*. \tag{40}$$

5.1.2 Distributions of T_{κ^*} and $T_\kappa, \kappa \neq \kappa^*$ under Uniform Random Sampling without Replacement

In this scenario, the plaintexts $P_1, \ldots, P_N$ are chosen according to uniform random sampling without replacement. As a result, $P_1, \ldots, P_N$ are no longer independent and correspondingly neither are $X_{\kappa,1}, \ldots, X_{\kappa,N}$. So, the analysis in the case for sampling with replacement needs to be modified. The discussion given below provides heuristic justification for the normality of the marginals $Q_{\kappa,\eta}$'s of the random vector Q_κ.

We first consider the distribution of T_{κ^*} in the scenario where $p_{\kappa^*}(\eta)$'s are random variables. A fraction $p_{\kappa^*}(\eta)$ of the 2^n possible plaintexts P satisfies the condition $X_{\kappa^*} = \eta$. So,

$$\Pr[Q_{\kappa^*,\eta} = \mathfrak{k}] = \frac{\binom{\lfloor p_{\kappa^*}(\eta)2^n \rfloor}{\mathfrak{k}} \binom{2^n - \lfloor p_{\kappa^*}(\eta)2^n \rfloor}{N-\mathfrak{k}}}{\binom{2^n}{N}}. \tag{41}$$

Under the general right key randomisation hypothesis it is assumed that $p_{\kappa^*}(\eta)$ follows $\mathcal{N}(p_\eta, s_0^2)$ so that the density function of $p_{\kappa^*}(\eta)$ is taken to be $\mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2)$. Then

$$\begin{aligned}\Pr[Q_{\kappa^*,\eta} \le x] &= \sum_{\mathfrak{k}\le x} \Pr[Q_{\kappa^*,\eta} = \mathfrak{k}] \\ &\approx \sum_{\mathfrak{k}\le x} \int_{-\infty}^{\infty} \frac{\binom{\lfloor \mathfrak{p}_\eta 2^n \rfloor}{\mathfrak{k}} \binom{2^n - \lfloor \mathfrak{p}_\eta 2^n \rfloor}{N-\mathfrak{k}}}{\binom{2^n}{N}} \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2) d\mathfrak{p} \\ &= \int_{-\infty}^{\infty} \left(\sum_{\mathfrak{k}\le x} \frac{\binom{\lfloor \mathfrak{p}_\eta 2^n \rfloor}{\mathfrak{k}} \binom{2^n - \lfloor \mathfrak{p}_\eta 2^n \rfloor}{N-\mathfrak{k}}}{\binom{2^n}{N}} \right) \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2) d\mathfrak{p}.\end{aligned}$$

An analysis along the lines of (33) to (34) using (27) shows that

$$\Pr[Q_{\kappa^*,\eta} \le x] \approx \int_{p_\eta-\theta_0}^{p_\eta+\theta_0} \left(\sum_{\mathfrak{k}\le x} \frac{\binom{\lfloor \mathfrak{p}_\eta 2^n \rfloor}{\mathfrak{k}} \binom{2^n - \lfloor \mathfrak{p}_\eta 2^n \rfloor}{N-\mathfrak{k}}}{\binom{2^n}{N}} \right) \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2) d\mathfrak{p}.$$

The sum within the integral can be seen to be the distribution function of the hypergeometric distribution $\mathsf{Hypergeometric}(N, 2^n, \lfloor \mathfrak{p}_\eta 2^n \rfloor)$. If $N/2^n = \mathfrak{t} \in (0,1)$, then the hypergeometric distribution approximately follows $\mathcal{N}(\mathfrak{p}_\eta N, N(1-\mathfrak{t})\mathfrak{p}_\eta(1-\mathfrak{p}_\eta))$ (see the appendix of [27] for a discussion) which using $\mathfrak{t} = N/2^n$ is equal to $\mathcal{N}(\mathfrak{p}_\eta N, N(1-N/2^n)\mathfrak{p}_\eta(1-\mathfrak{p}_\eta))$.

For $\mathfrak{p}_\eta \in [p_\eta - \theta_0, p_\eta + \theta_0]$, from (29) the normal distribution $\mathcal{N}(\mathfrak{p}_\eta N, N(1-N/2^n)\mathfrak{p}_\eta(1-\mathfrak{p}_\eta))$ is approximated as $\mathcal{N}(N\mathfrak{p}_\eta, N2^{-\ell}(1-N/2^n)(1-2^{-\ell}))$. The approximation is meaningful in the mentioned range of $\mathfrak{p}_\eta$ and it is not valid for values of $\mathfrak{p}_\eta$ close to 0 or 1.

$$\begin{aligned}\Pr[Q_{\kappa^*,\eta} \le x] &\approx \int_{p_\eta-\theta_0}^{p_\eta+\theta_0} \left(\int_{-\infty}^{x} \mathfrak{f}(x; N\mathfrak{p}_\eta, N2^{-\ell}(1-N/2^n)(1-2^{-\ell}))\ dx \right) \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2)\ d\mathfrak{p} \\ &\le \int_{-\infty}^{\infty} \left(\int_{-\infty}^{x} \mathfrak{f}(x; N\mathfrak{p}_\eta, N2^{-\ell}(1-N/2^n)(1-2^{-\ell}))\ dx \right) \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2)\ d\mathfrak{p} \\ &= \int_{-\infty}^{x} \left(\int_{-\infty}^{\infty} \mathfrak{f}(x; N\mathfrak{p}_\eta, N2^{-\ell}(1-N/2^n)(1-2^{-\ell})) \mathfrak{f}(\mathfrak{p}_\eta; p_\eta, s_0^2)\ d\mathfrak{p} \right) dx \\ &= \int_{-\infty}^{x} \mathfrak{f}(x; Np_\eta, s_0^2 N^2 + N2^{-\ell}(1-N/2^n)(1-2^{-\ell}))dx.\end{aligned}$$

The last equality is based on compound normal and we refer to the appendix of [27] for a proof. So, $Q_{\kappa^*,\eta}$ approximately follows $\mathcal{N}(Np_\eta, N^2 s_0^2 + N2^{-\ell}(1-N/2^n)(1-2^{-\ell}))$ and since $Z_{\kappa^*,\eta} = Q_{\kappa^*,\eta}/N - 2^{-\ell}$ we have that the distribution of $Z_{\kappa^*,\eta}$ is approximately given as follows:

$$Z_{\kappa^*,\eta} \sim \mathcal{N}\left(\epsilon_\eta, s_0^2 + \frac{1}{2^\ell}\left(\frac{1}{N} - \frac{1}{2^n}\right)\left(1 - \frac{1}{2^\ell}\right)\right). \tag{42}$$

For T_κ with $\kappa \ne \kappa^*$, we need to consider the general wrong key randomisation hypothesis where $q_{\kappa,\kappa^*}(\eta)$ is modelled as a random variable following $\mathcal{N}(2^{-\ell}, s_1^2)$. In this case, it is required to use (30) and (31) instead of (27) and (28) respectively. In particular, as in the case of sampling with replacement, we note that for $\mathfrak{q}_\eta \in [2^{-\ell} - \vartheta_1, 2^{-\ell} + \vartheta_1]$, it is required to approximate $\mathcal{N}(N\mathfrak{q}_\eta, N(1-N/2^n)\mathfrak{q}_\eta(1-\mathfrak{q}_\eta))$ by $\mathcal{N}(N\mathfrak{q}_\eta, N2^{-\ell}(1-N/2^n)(1-2^{-\ell}))$, i.e., $\mathfrak{q}_\eta(1-\mathfrak{q}_\eta) \approx 2^{-\ell}(1-2^{-\ell})$. The validity of this follows from (31) and the approximation is not valid for values of $\mathfrak{q}_\eta$ near to 0 or 1. With these approximations, the resulting analysis shows the following approximate distribution:

$$Z_{\kappa,\eta} \sim \mathcal{N}\left(0, s_1^2 + \frac{1}{2^\ell}\left(\frac{1}{N} - \frac{1}{2^n}\right)\left(1 - \frac{1}{2^\ell}\right)\right), \quad \kappa \ne \kappa^*. \tag{43}$$

Like in the case of sampling with replacement, appropriate heuristic assumptions based on the conditions of Theorem 6 in Appendix A.1 are needed to obtain approximate distributions of T_{κ^*} and $T_\kappa, \kappa \neq \kappa^*$.

$$\frac{T_{\kappa^*}}{N\left(2^\ell s_0^2 + \left(\frac{1}{N} - \frac{1}{2^n}\right)\left(1 - \frac{1}{2^\ell}\right)\right)} \sim \chi^2_{2^\ell - 1}(\delta) \tag{44}$$

$$\frac{T_\kappa}{N\left(2^\ell s_1^2 + \left(\frac{1}{N} - \frac{1}{2^n}\right)\left(1 - \frac{1}{2^\ell}\right)\right)} \sim \chi^2_{2^\ell - 1}, \quad \kappa \neq \kappa^*; \tag{45}$$

where

$$\delta = \sum_{\eta \in \{0,1\}^\ell} \frac{\epsilon_\eta^2}{s_0^2 + \frac{1}{2^\ell}\left(\frac{1}{N} - \frac{1}{2^n}\right)\left(1 - \frac{1}{2^\ell}\right)} = \frac{NC^{(\mathrm{md})}}{Ns_0^2 2^\ell + \left(1 - \frac{N}{2^n}\right)\left(1 - \frac{1}{2^\ell}\right)}. \tag{46}$$

5.2 Multiple Case

The test statistic is T_κ which is given in (13). This is defined from the random variables $Y_{\kappa,1}, \ldots, Y_{\kappa,\ell}$. The distribution of $Y_{\kappa,i}$ is in turn based on the distribution of $p_{\kappa^*,i}$ for $\kappa = \kappa^*$, or on the distribution of $q_{\kappa,\kappa^*,i}$ for $\kappa \neq \kappa^*$. Given the distributions of $p_{\kappa^*,i}$ and $q_{\kappa,\kappa^*,i}$ modelled by the two general multiple key randomisation hypotheses, the requirement is to obtain approximations of the distributions of $Y_{\kappa^*,i}$ and $Y_{\kappa,i}$ and hence of T_{κ^*} and T_κ respectively.

In the setting of multiple linear approximation, the random variables $Y_{\kappa,1}, \ldots, Y_{\kappa,\ell}$ are assumed to be independent. Unlike the case of multidimensional cryptanalysis, it is not required to make the heuristic assumption that $Y_\kappa = (Y_{\kappa,1}, \ldots, Y_{\kappa,\ell})$ follows a multivariate normal and consequently, it is not required to make the heuristic assumption that the variance-covariance matrix of Y_κ satisfies the conditions of Theorem 6 of Appendix A.1 to assume that T_κ follows a chi-squared distribution.

The distributions of $Y_{\kappa^*,i}$ and $Y_{\kappa,i}$, $\kappa \neq \kappa^*$ depend on whether $P_1, \ldots, P_N$ are chosen with or without replacement. In both cases, the analysis is essentially the same as that for the single linear approximation done in [27]. So, we skip the details.

5.2.1 Distributions of T_{κ^*} and $T_\kappa, \kappa \neq \kappa^*$ under Uniform Random Sampling with Replacement

In this case, $P_1, \ldots, P_N$ are chosen under uniform random sampling with replacement so that $P_1, \ldots, P_N$ are assumed to be independent and uniformly distributed over $\{0,1\}^n$. The form of the test statistic is given by (13) which is defined from the random variables $Y_{\kappa,i}$. The distributions of $Y_{\kappa^*,i}$ and $Y_{\kappa,i}$, $\kappa \neq \kappa^*$ are determined by the distributions of $p_{\kappa^*,i}$'s and $q_{\kappa,\kappa^*,i}$'s, respectively. Proceeding as in Section 5.1 of [27], it can be heuristically shown that the following approximately holds.

$$Y_{\kappa^*,i} \sim \mathcal{N}\left(Np_i, N^2 s_0^2 + \frac{N}{4}\right) \quad \text{and} \quad Y_{\kappa,i} \sim \mathcal{N}\left(\frac{N}{2}, N^2 s_1^2 + \frac{N}{4}\right). \tag{47}$$

First consider T_{κ^*}. Since it is assumed that each of the ℓ linear approximations are independent, the $Y_{\kappa^*,i}$'s are also independent. So, the random variable

$$\sum_{i=1}^{\ell} \frac{(Y_{\kappa^*,i} - N/2)^2}{N^2 s_0^2 + \frac{N}{4}}$$

is equal to the sum of squares of independent normal variates, which we know follows a non-central chi-squared distribution if the mean of at least one of the normal distribution is non-zero. Therefore, we have

$$\frac{T_{\kappa^*}}{4Ns_0^2 + 1} \sim \chi^2_\ell(\delta), \tag{48}$$

where

$$\delta \;=\; \sum_{i=1}^{\ell} \frac{N^2\epsilon_i^2}{N^2 s_0^2 + \frac{N}{4}} = \frac{N\sum_{i=1}^{\ell} 4\epsilon_i^2}{4Ns_0^2+1} = \frac{NC^{(\mathrm{m})}}{4Ns_0^2+1}.$$

Similarly, it can be heuristically argued that for all $\kappa \neq \kappa^*$,

$$\frac{T_\kappa}{4Ns_1^2+1} \sim \chi^2_\ell. \tag{49}$$

5.2.2 Distributions of T_{κ^*} and $T_\kappa, \kappa \neq \kappa^*$ under Uniform Random Sampling without Replacement

Proceeding as in Section 5.2 of [27], it can be heuristically argued that the following approximately holds.

$$Y_{\kappa^*,i} \sim \mathcal{N}\left(Np_i, N^2 s_0^2 + \left(1-\frac{N}{2^n}\right)\frac{N}{4}\right) \quad \text{and} \quad Y_{\kappa,i} \sim \mathcal{N}\left(\frac{N}{2}, N^2 s_1^2 + \left(1-\frac{N}{2^n}\right)\frac{N}{4}\right). \tag{50}$$

So,

$$T_{\kappa^*} = \sum_{i=1}^{\ell} \frac{\left(Y_{\kappa*,i} - N/2\right)^2}{N/4} = \left(4Ns_0^2 + \left(1-\frac{N}{2^n}\right)\right)\sum_{i=1}^{\ell} \frac{\left(Y_{\kappa*,i} - N/2\right)^2}{N^2 s_0^2 + \left(1-\frac{N}{2^n}\right)\frac{N}{4}}.$$

Since it is assumed that each of the ℓ linear approximations are independent, we have, by the argument given in the preceding section,

$$\frac{T_{\kappa^*}}{4Ns_0^2 + \left(1-\frac{N}{2^n}\right)} \sim \chi^2_\ell(\delta), \tag{51}$$

where

$$\delta \;=\; \sum_{i=1}^{\ell} \frac{N^2\epsilon_i^2}{\left(N^2 s_0^2 + \left(1-\frac{N}{2^n}\right)\frac{N}{4}\right)} = \frac{N\sum_{i=1}^{\ell} 4\epsilon_i^2}{4Ns_0^2 + \left(1-\frac{N}{2^n}\right)} = \frac{NC^{(\mathrm{m})}}{4Ns_0^2 + \left(1-\frac{N}{2^n}\right)}.$$

Similarly, it can be heuristically argued that for all $\kappa \neq \kappa^*$,

$$\frac{T_\kappa}{4Ns_1^2 + \left(1-\frac{N}{2^n}\right)} \sim \chi^2_\ell. \tag{52}$$

6 Success Probability under General Key Randomisation Hypotheses

We separately consider the two cases of multidimensional and multiple linear cryptanalysis.

6.1 Multidimensional Case

The distributions of T_{κ^*} and T_κ for $\kappa \neq \kappa^*$ are respectively given by (38) and (40) for the case of sampling with replacement and are given by (44) and (45) for the case of sampling without replacement. These expressions can be compactly expressed in the following form:

$$\frac{T_{\kappa^*}}{N(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})} \sim \chi^2_{2^\ell-1}(\delta_{(\mathrm{md})}); \qquad \frac{T_\kappa}{N(2^\ell s_1^2 + \sigma^2_{(\mathrm{md})})} \sim \chi^2_{2^\ell-1}, \quad \text{for } \kappa \neq \kappa^*; \tag{53}$$

where

$$\sigma^2_{(\mathrm{md})} \;=\; \begin{cases} \frac{1}{N}\left(1-\frac{1}{2^\ell}\right) & \text{for sampling with replacement;} \\ \left(\frac{1}{N}-\frac{1}{2^n}\right)\left(1-\frac{1}{2^\ell}\right) & \text{for sampling without replacement,} \end{cases} \tag{54}$$

and

$$\delta_{(\mathrm{md})} = \begin{cases} \frac{NC^{(\mathrm{md})}}{N2^\ell s_0^2+(1-2^{-\ell})} & \text{for sampling with replacement;} \\ \frac{NC^{(\mathrm{md})}}{Ns_0^2 2^\ell+\left(1-\frac{N}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)} & \text{for sampling without replacement.} \end{cases} \quad (55)$$

Recall that for sampling with replacement, we have

$$\delta_{(\mathrm{md})} = \frac{NC^{(\mathrm{md})}}{N2^\ell s_0^2 + (1-2^{-\ell})} = \frac{C^{(\mathrm{md})}}{2^\ell s_0^2 + \frac{(1-2^{-\ell})}{N}}$$

which is an increasing function of N. Similarly, for sampling without replacement we have

$$\delta_{(\mathrm{md})} = \frac{NC^{(\mathrm{md})}}{Ns_0^2 2^\ell + \left(1-\frac{N}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)} = \frac{C^{(\mathrm{md})}}{s_0^2 2^\ell + \left(\frac{1}{N}-\frac{1}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)}$$

which is again an increasing function of N. Since, $\delta_{(\mathrm{md})}$ increases with N, we can approximate the non-central chi-square distribution by a normal distribution with mean $(2^\ell - 1) + \delta_{(\mathrm{md})}$ and variance $2((2^\ell - 1) + 2\delta_{(\mathrm{md})})$ (see Theorem 7 of Appendix A.2). Then T_{κ^*} approximately follows a normal distribution with mean $N(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})((2^\ell - 1) + \delta_{(\mathrm{md})})$ and variance $2N^2(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})^2((2^\ell - 1) + 2\delta_{(\mathrm{md})})$. Substituting $\sigma_0^2 = 2N^2(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})^2((2^\ell - 1) + 2\delta_{(\mathrm{md})})$, $\mu_0 = N(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})((2^\ell - 1) + \delta_{(\mathrm{md})})$, $\omega = N(2^\ell s_1^2 + \sigma^2_{(\mathrm{md})})$ and $\nu = 2^\ell - 1$ in Theorem 1, we obtain the following result.

Theorem 2. *Let $\kappa^* \in \{0,1\}^m$. For $\kappa \in \{0,1\}^m$, let T_κ be 2^m random variables, where*

$$\begin{aligned} T_{\kappa^*} &\sim \mathcal{N}(N(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})((2^\ell - 1) + \delta_{(\mathrm{md})}), 2N^2(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})^2((2^\ell - 1) + 2\delta_{(\mathrm{md})})); \\ T_\kappa/N(2^\ell s_1^2 + \sigma^2_{(\mathrm{md})}) &\sim \chi^2_{2^\ell-1}, \text{ for } \kappa \neq \kappa^*; \end{aligned}$$

$\sigma^2_{(\mathrm{md})}$ and $\delta_{(\mathrm{md})}$ are given by (54) and (55) respectively.

Suppose the hypothesis test given in (18) is applied to T_κ for all $\kappa \in \{0,1\}^m$. Let $P_S = 1 - \Pr[\text{Type-1 error}]$ and the expected number of times that Type-2 errors occurs is 2^{m-a}. Then

$$P_S = \Phi\left(\frac{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})((2^\ell - 1) + \delta_{(\mathrm{md})}) - (2^\ell s_1^2 + \sigma^2_{(\mathrm{md})})\gamma}{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})\sqrt{2((2^\ell - 1) + 2\delta_{(\mathrm{md})})}}\right) \quad (56)$$

where $\gamma = \Psi^{-1}\left(1 - \frac{2^{m-a-1}}{2^m-1}\right)$.

6.2 Multiple Case

The distributions of T_{κ^*} and T_κ for $\kappa \neq \kappa^*$ are respectively given by (48) and (49) for the case of sampling with replacement and are given by (51) and (52) for the case of sampling without replacement. These expressions can be compactly expressed in the following form:

$$\frac{T_{\kappa^*}}{N(4s_0^2 + \sigma^2_{(\mathrm{m})})} \sim \chi^2_\ell(\delta_{(\mathrm{m})}); \qquad \frac{T_\kappa}{N(4s_1^2+\sigma^2_{(\mathrm{m})})} \sim \chi^2_\ell, \quad \text{for } \kappa \neq \kappa^*; \quad (57)$$

where

$$\sigma^2_{(\mathrm{m})} = \begin{cases} \frac{1}{N} & \text{for sampling with replacement;} \\ \frac{1}{N} - \frac{1}{2^n} & \text{for sampling without replacement,} \end{cases} \quad (58)$$

and

$$\delta_{(\mathrm{m})} = \begin{cases} \frac{NC^{(\mathrm{m})}}{4Ns_0^2+1} & \text{for sampling with replacement;} \\ \frac{NC^{(\mathrm{m})}}{4Ns_0^2+\left(1-\frac{N}{2^n}\right)} & \text{for sampling without replacement.} \end{cases} \tag{59}$$

Recall that for sampling without replacement, we have

$$\delta_{(\mathrm{m})} = \frac{NC^{(\mathrm{m})}}{4Ns_0^2+\left(1-\frac{N}{2^n}\right)} = \frac{C^{(\mathrm{m})}}{4s_0^2+\left(\frac{1}{N}-\frac{1}{2^n}\right)}$$

which is an increasing function of N. Similarly, for sampling with replacement we have

$$\delta_{(\mathrm{m})} = \frac{NC^{(\mathrm{m})}}{4Ns_0^2+1} = \frac{C^{(\mathrm{m})}}{4s_0^2+\frac{1}{N}}$$

which is again an increasing function of N. Since, $\delta_{(\mathrm{m})}$ increases with N, we can approximate the non-central chi-square distribution by a normal distribution with mean $(\ell+\delta_{(\mathrm{m})})$ and variance $2(\ell+2\delta_{(\mathrm{m})})$ (see Theorem 7 of Appendix A.2). Then T_{κ^*} approximately follow a normal distribution with mean $N(4s_0^2+\sigma_{(\mathrm{m})}^2)(\ell+\delta_{(\mathrm{m})})$ and variance $2N^2(4s_0^2+\sigma_{(\mathrm{m})}^2)^2(\ell+2\delta_{(\mathrm{m})})$. Substituting $\sigma_0^2 = 2N^2(4s_0^2+\sigma_{(\mathrm{m})}^2)^2(\ell+2\delta_{(\mathrm{m})})$, $\mu_0 = N(4s_0^2+\sigma_{(\mathrm{m})}^2)(\ell+\delta_{(\mathrm{m})})$, $\omega = N(4s_1^2+\sigma_{(\mathrm{m})}^2)$ and $\nu = \ell$ in Theorem 1, we obtain the following result.

Theorem 3. *Let $\kappa^* \in \{0,1\}^m$. For $\kappa \in \{0,1\}^m$, let T_κ be 2^m random variables, where*

$$\begin{aligned} T_{\kappa^*} &\sim \mathcal{N}(N(4s_0^2+\sigma_{(\mathrm{m})}^2)(\ell+\delta_{(\mathrm{m})}), 2N^2(4s_0^2+\sigma_{(\mathrm{m})}^2)^2(\ell+2\delta_{(\mathrm{m})})); \\ T_\kappa/N(4s_1^2+\sigma_{(\mathrm{m})}^2) &\sim \chi_\ell^2, \text{ for } \kappa \neq \kappa^*; \end{aligned}$$

$\sigma_{(\mathrm{m})}$ and $\delta_{(\mathrm{m})}$ are given by (59) and (58) respectively. Suppose the hypothesis test given in (18) is applied to T_κ for all $\kappa \in \{0,1\}^m$. Let $P_S = 1 - \Pr[\text{Type-1 error}]$ and the expected number of times that Type-2 errors occurs is 2^{m-a}. Then

$$P_S = \Phi\left(\frac{(4s_0^2+\sigma_{(\mathrm{m})}^2)(\ell+\delta_{(\mathrm{m})}) - (4s_1^2+\sigma_{(\mathrm{m})}^2)\gamma}{(4s_0^2+\sigma_{(\mathrm{m})}^2)\sqrt{2(\ell+2\delta_{(\mathrm{m})})}}\right) \tag{60}$$

where $\gamma = \Psi^{-1}\left(1-\frac{2^{m-a-1}}{2^m-1}\right)$.

7 Success Probability Under Particular Key Randomisation Hypotheses

In this section we give the expressions for success probability of multidimensional/multiple linear cryptanalysis under different settings, namely, multidimensional or multiple; sampling with or without replacement; and whether standard or adjusted key randomisation hypothesis are used for the right or the wrong key. To differentiate between these cases, we will use superscripts to P_S denoting the different possible cases. The notation for these superscripts are as follows.

1. The superscripts md and m will denote multidimensional and multiple linear cryptanalysis respectively.
2. The superscripts wr and wor will denote namely sampling with replacement and sampling without replacement respectively.

3. The superscripts std, adj, radj and wadj will denote the different combinations of the key randomisation hypotheses.
   - The superscript std will denote that the standard key randomisation hypothesis is considered for both right and wrong key.
   - The superscript adj will denote that the adjusted key randomisation hypothesis is considered for both right and wrong key.
   - The superscript radj will denote the adjusted right key randomisation hypothesis and the standard wrong key randomisation hypothesis.
   - The superscript wadj will denote the adjusted wrong key randomisation hypothesis and the standard right key randomisation hypothesis.

So, there are 16 possible cases. For each of these cases, we state the corresponding expressions for the success probabilities.

7.1 Success Probability for Multidimensional Linear Cryptanalysis

Let $P_S^{(\mathrm{md,wr},\cdot)}$ denote the success probability of multidimensional linear cryptanalysis when sampling with replacement is used and let $P_S^{(\mathrm{md,wor},\cdot)}$ denote the success probability of multidimensional linear cryptanalysis when sampling without replacement is used. The third slot is for the type of key randomisation hypothesis used, i.e., the third slot can be filled up in 4 ways, namely std, adj, radj and wadj. Notice that std, adj, radj and wadj influences only the values of s_0^2 and s_1^2 of (56). Therefore we can get the values of $P_S^{(\mathrm{m,wr},\cdot)}$ and $P_S^{(\mathrm{m,wor},\cdot)}$ by using the corresponding expressions for σ from (54) and (55) in (56).

$$P_S^{(\mathrm{md,wr},\cdot)} = \Phi\left(\frac{\left(2^\ell s_0^2+\frac{1}{N}\left(1-\frac{1}{2^\ell}\right)\right)\left((2^\ell-1)+\frac{NC^{(\mathrm{md})}}{N2^\ell s_0^2+(1-2^{-\ell})}\right)-\left(2^\ell s_1^2+\frac{1}{N}\left(1-\frac{1}{2^\ell}\right)\right)\gamma}{\left(2^\ell s_0^2+\frac{1}{N}\left(1-\frac{1}{2^\ell}\right)\right)\sqrt{2\left((2^\ell-1)+\frac{2NC^{(\mathrm{md})}}{N2^\ell s_0^2+(1-2^{-\ell})}\right)}}\right); \tag{61}$$

$$P_S^{(\mathrm{md,wor},\cdot)} = \Phi\left(\frac{\left(2^\ell s_0^2+\left(\frac{1}{N}-\frac{1}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)\right)\left((2^\ell-1)+\frac{NC^{(\mathrm{md})}}{Ns_0^2 2^\ell+\left(1-\frac{N}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)}\right)-\left(2^\ell s_1^2+\left(\frac{1}{N}-\frac{1}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)\right)\gamma}{\left(2^\ell s_0^2+\left(\frac{1}{N}-\frac{1}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)\right)\sqrt{2\left((2^\ell-1)+\frac{2NC^{(\mathrm{md})}}{Ns_0^2 2^\ell+\left(1-\frac{N}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)}\right)}}\right) \tag{62}$$

Remarks:

1. If $N \ll 2^n$, then $P_S^{(\mathrm{md,wor},\cdot)} \approx P_S^{(\mathrm{md,wr},\cdot)}$. So, the expression for $P_S^{(\mathrm{md,wor},\cdot)}$ given by (62) becomes useful only when the fraction $N/2^n$ is non-negligible.
2. In the case of sampling with replacement, due to the birthday paradox, having N to be greater than $2^{n/2}$ is not really useful, since repetitions will begin to occur.

7.1.1 Success Probability Under Standard Key Randomisation Hypotheses

Let $P_S^{(\mathrm{md,wr,std})}$ and $P_S^{(\mathrm{md,wor,std})}$ be the success probabilities of multidimensional linear cryptanalysis for both standard multidimensional right and wrong key randomisation hypotheses corresponding to the situations where plaintexts are chosen with and without replacement respectively. As discussed in Section 4.1, the standard key randomisation hypotheses is obtained from the general key randomisation hypothesis by letting $s_0 \downarrow 0$ and $s_1 \downarrow 0$. Using these conditions in (61) and (62) lead to the following expressions for the success probabilities of multidimensional linear cryptanalysis in the two cases of sampling with and without replacement.

$$P_S^{(\mathrm{md,wr,std})} = \Phi\left(\frac{\left((2^\ell-1)+\frac{NC^{(\mathrm{md})}}{(1-2^{-\ell})}\right)-\gamma}{\sqrt{2\left((2^\ell-1)+\frac{2NC^{(\mathrm{md})}}{(1-2^{-\ell})}\right)}}\right) \tag{63}$$

$$P_S^{(\mathrm{md,wor,std})} = \Phi\left(\frac{\left((2^\ell-1)+\frac{NC^{(\mathrm{md})}}{\left(1-\frac{N}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)}\right)-\gamma}{\sqrt{2\left((2^\ell-1)+\frac{2NC^{(\mathrm{md})}}{\left(1-\frac{N}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)}\right)}}\right). \tag{64}$$

Success probability in [16]: Hermelin et al [16] had obtained an expression for the success probability under the standard multidimensional key randomisation hypotheses and under the assumption that $P_1, \ldots, P_N$ are chosen uniformly with replacements. Assuming that $1 - 2^{-\ell} \approx 1$, the expression for $P_S^{(\mathrm{md,wr,std})}$ given by (63) becomes exactly the same as equation (6.8) of [25]. It was shown in [25] that under few further approximations this expression becomes exactly the same as the expression given in [16, Section 5.1].

To the best of our knowledge, no prior work has analysed the success probability of multidimensional linear cryptanalysis with the standard key randomisation hypotheses and under the condition where $P_1, \ldots, P_N$ are chosen uniformly without replacement. So, the expression for $P_S^{(\mathrm{md,wor,std})}$ given by (64) is the first such result.

7.1.2 Success Probability Under Adjusted Wrong Key Randomisation Hypothesis

Let $P_S^{(\mathrm{md,wr,wadj})}$ and $P_S^{(\mathrm{md,wor,wadj})}$ be the success probabilities of multidimensional linear cryptanalysis for adjusted multidimensional wrong key randomisation hypothesis and standard multidimensional right key randomisation hypothesis corresponding to the situations where plaintexts are chosen with and without replacement respectively.

Setting $s_0^2 \downarrow 0$ converts the general right key randomisation hypothesis to the standard right key randomisation hypothesis. Also, we let $s_1^2 = \frac{1}{2^{n+\ell}}\left(1 - \frac{1}{2^\ell}\right)$, so that the general wrong key randomisation hypothesis simplifies to the adjusted wrong key randomisation hypothesis. Using the conditions for s_0 and s_1 in (61) and (62) provides the following expressions for the success probabilities of multidimensional linear cryptanalysis in the two cases

of sampling with and without replacement.

$$P_S^{(\mathrm{md,wr,wadj})} = \Phi\left(\frac{\left((2^\ell-1)+\frac{NC^{(\mathrm{md})}}{(1-2^{-\ell})}\right)-\left(1+\frac{N}{2^n}\right)\gamma}{\sqrt{2\left((2^\ell-1)+\frac{2NC^{(\mathrm{md})}}{(1-2^{-\ell})}\right)}}\right); \tag{65}$$

$$P_S^{(\mathrm{md,wor,wadj})} = \Phi\left(\frac{\left(1-\frac{N}{2^n}\right)\left((2^\ell-1)+\frac{NC^{(\mathrm{md})}}{\left(1-\frac{N}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)}\right)-\gamma}{\left(1-\frac{N}{2^n}\right)\sqrt{2\left((2^\ell-1)+\frac{2NC^{(\mathrm{md})}}{\left(1-\frac{N}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)}\right)}}\right). \tag{66}$$

To the best of our knowledge, no prior work has analysed the success probability of multidimensional linear cryptanalysis for the adjusted wrong key randomisation hypothesis and standard multidimensional right key randomisation hypothesis corresponding to the situation where plaintexts $P_1,\ldots,P_N$ are chosen with and without replacement, respectively. So, the expressions for $P_S^{(\mathrm{md,wr,wadj})}$ and $P_S^{(\mathrm{md,wor,wadj})}$ given by (65) and (66) are the first such results.

7.1.3 Success Probability Under Adjusted Right Key Randomisation Hypothesis

Let $P_S^{(\mathrm{md,wr,radj})}$ and $P_S^{(\mathrm{md,wor,radj})}$ be the success probabilities of multidimensional linear cryptanalysis for adjusted right key randomisation hypothesis and standard wrong key randomisation hypothesis corresponding to the situations where plaintexts are chosen with and without replacement respectively.

Setting $s_0^2=\frac{C-C^{(\mathrm{md})}}{2^{2\ell}}$ converts the general multidimensional right key randomisation hypothesis to the adjusted multidimensional right key randomisation hypothesis. Also, we let $s_1^2\downarrow 0$, so that the general multidimensional wrong key randomisation hypothesis simplifies to the standard multidimensional wrong key randomisation hypothesis. Using the conditions for s_0 and s_1 in (61) and (62) provides the following expressions for the success probabilities of multidimensional linear cryptanalysis in the two cases of sampling with and without replacement.

$$P_S^{(\mathrm{md,wr,radj})} = \Phi\left(\frac{\left(\frac{C-C^{(\mathrm{md})}}{2^\ell}+\frac{1}{N}\left(1-\frac{1}{2^\ell}\right)\right)\left((2^\ell-1)+\frac{NC^{(\mathrm{md})}}{\frac{N(C-C^{(\mathrm{md})})}{2^\ell}+(1-2^{-\ell})}\right)-\left(\frac{1}{N}\left(1-\frac{1}{2^\ell}\right)\right)\gamma}{\left(\frac{C-C^{(\mathrm{md})}}{2^\ell}+\frac{1}{N}\left(1-\frac{1}{2^\ell}\right)\right)\sqrt{2\left((2^\ell-1)+\frac{2NC^{(\mathrm{md})}}{\frac{N(C-C^{(\mathrm{md})})}{2^\ell}+(1-2^{-\ell})}\right)}}\right); \tag{67}$$

$$P_S^{(\mathrm{md,wor,radj})} = \Phi\left(\frac{\left((2^\ell-1)+\frac{NC^{(\mathrm{md})}}{\frac{N(C-C^{(\mathrm{md})})}{2^\ell}+\left(1-\frac{N}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)}\right)-\frac{\left(\frac{1}{N}-\frac{1}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)\gamma}{\frac{C-C^{(\mathrm{md})}}{2^\ell}+\left(\frac{1}{N}-\frac{1}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)}}{\sqrt{2\left((2^\ell-1)+\frac{2NC^{(\mathrm{md})}}{\frac{N(C-C^{(\mathrm{md})})}{2^\ell}+\left(1-\frac{N}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)}\right)}}\right). \tag{68}$$

The case of adjusted right key randomisation hypothesis and standard wrong key randomisation hypothesis was considered in [17] where sampling with replacement is used. The work showed that the capacity follows a gamma distribution but, did not provide an expression for the success probability. To the best of our knowledge, no prior work has considered sampling without replacement for this case. So, the expressions for $P_S^{(\mathrm{md,wr,radj})}$ and $P_S^{(\mathrm{md,wor,radj})}$ given by (67) and (68) are the first such results.

7.1.4 Success Probability Under Adjusted Key Randomisation Hypothesis

Let $P_S^{(\mathrm{md,wr,adj})}$ and $P_S^{(\mathrm{md,wor,adj})}$ be the success probabilities of multidimensional linear cryptanalysis for both adjusted multidimensional right and wrong key randomisation hypothesis corresponding to the situations where plaintexts are chosen with and without replacement respectively.

Setting $s_1^2 = \frac{1}{2^{n+\ell}}\left(1-\frac{1}{2^\ell}\right)$ converts the general multidimensional wrong key randomisation hypothesis to the adjusted multidimensional wrong key randomisation hypothesis. Also, we let $s_0^2 = \frac{C-C^{(\mathrm{md})}}{2^{2\ell}}$, so that the general multidimensional right key randomisation hypothesis simplifies to the adjusted multidimensional right key randomisation hypothesis. Using the conditions for s_0 and s_1 in (61) and (62) provides the following expressions for the success probabilities in the two cases of sampling with and without replacement.

$$P_S^{(\mathrm{md,wr,adj})} = \Phi\left(\frac{\left(\frac{C-C^{(\mathrm{md})}}{2^\ell}+\frac{1}{N}\left(1-\frac{1}{2^\ell}\right)\right)\left((2^\ell-1)+\frac{NC^{(\mathrm{md})}}{\frac{N(C-C^{(\mathrm{md})})}{2^\ell}+(1-2^{-\ell})}\right)-\left(\frac{1}{N}+\frac{1}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)\gamma}{\left(\frac{C-C^{(\mathrm{md})}}{2^\ell}+\frac{1}{N}\left(1-\frac{1}{2^\ell}\right)\right)\sqrt{2\left((2^\ell-1)+\frac{2NC^{(\mathrm{md})}}{\frac{N(C-C^{(\mathrm{md})})}{2^\ell}+(1-2^{-\ell})}\right)}}\right); \tag{69}$$

$$P_S^{(\mathrm{md,wor,adj})} = \Phi\left(\frac{\left(\frac{C-C^{(\mathrm{md})}}{2^\ell}+\left(\frac{1}{N}-\frac{1}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)\right)\left((2^\ell-1)+\frac{NC^{(\mathrm{md})}}{\frac{N(C-C^{(\mathrm{md})})}{2^\ell}+\left(1-\frac{N}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)}\right)-\frac{1}{N}\left(1-\frac{1}{2^\ell}\right)\gamma}{\left(\frac{C-C^{(\mathrm{md})}}{2^\ell}+\left(\frac{1}{N}-\frac{1}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)\right)\sqrt{2\left((2^\ell-1)+\frac{2NC^{(\mathrm{md})}}{\frac{N(C-C^{(\mathrm{md})})}{2^\ell}+\left(1-\frac{N}{2^n}\right)\left(1-\frac{1}{2^\ell}\right)}\right)}}\right). \tag{70}$$

Expressions for the success probability with the adjusted multidimensional key randomisation hypothesis under both sampling with and without repetitions were obtained in [7]. The expressions given in [7] hold for those values of ℓ for which the central chi-square distribution can be approximated by a normal.

We consider applying the approximations made in [7] to the expressions for P_S given by (69) and (70).

Assume that $1-2^{-\ell} \approx 1$, $C^{(\mathrm{md})} = 0$ and $C = \frac{\lambda(2^\ell - 1)}{2^n}$, where $\lambda \geq 1$. Then from (69) and (70), we have

$$\begin{aligned}
P_S^{(\mathrm{md,wr,adj})} &\approx \Phi\left(\frac{\left(\frac{\lambda(2^\ell-1)}{2^{n+\ell}} + \frac{1}{N}\right)(2^\ell - 1) - \left(\frac{1}{N} + \frac{1}{2^n}\right)\gamma}{\left(\frac{\lambda(2^\ell-1)}{2^{n+\ell}} + \frac{1}{N}\right)\sqrt{2(2^\ell-1)}}\right) \\
&\approx \Phi\left(\frac{\left(\frac{\lambda}{2^n} + \frac{1}{N}\right)(2^\ell - 1) - \left(\frac{1}{N} + \frac{1}{2^n}\right)\gamma}{\left(\frac{\lambda}{2^n} + \frac{1}{N}\right)\sqrt{2(2^\ell-1)}}\right) \\
&= \Phi\left(\frac{(\lambda N + 2^n)(2^\ell - 1) - (N + 2^n)\gamma}{(\lambda N + 2^n)\sqrt{2(2^\ell-1)}}\right); \\
P_S^{(\mathrm{md,wor,adj})} &\approx \Phi\left(\frac{\left(\frac{\lambda(2^\ell-1)}{2^{n+\ell}} + \left(\frac{1}{N} - \frac{1}{2^n}\right)\right)(2^\ell - 1) - \frac{\gamma}{N}}{\left(\frac{\lambda(2^\ell-1)}{2^{n+\ell}} + \left(\frac{1}{N} - \frac{1}{2^n}\right)\right)\sqrt{2(2^\ell-1)}}\right) \\
&\approx \Phi\left(\frac{\left(\frac{\lambda}{2^n} + \left(\frac{1}{N} - \frac{1}{2^n}\right)\right)(2^\ell - 1) - \frac{\gamma}{N}}{\left(\frac{\lambda}{2^n} + \left(\frac{1}{N} - \frac{1}{2^n}\right)\right)\sqrt{2(2^\ell-1)}}\right) \\
&\approx \Phi\left(\frac{\left(\frac{\lambda-1}{2^n} + \frac{1}{N}\right)(2^\ell - 1) - \frac{\gamma}{N}}{\left(\frac{\lambda-1}{2^n} + \frac{1}{N}\right)\sqrt{2(2^\ell-1)}}\right) \\
&= \Phi\left(\frac{(N(\lambda-1) + 2^n)(2^\ell - 1) - 2^n\gamma}{(N(\lambda-1) + 2^n)\sqrt{2(2^\ell-1)}}\right)
\end{aligned}$$

As mentioned earlier, [7] approximates the central chi-square distribution by a normal distribution. For this, it is required to replace γ by $(2^\ell - 1) + \sqrt{2(2^\ell - 1)}\varphi_a$, where $\varphi_a = \Phi^{-1}(1 - 2^{-a})$. Using this in the above gives

$$\begin{aligned}
P_S^{(\mathrm{md,wr,adj})} &\approx \Phi\left(\frac{N(\lambda-1)\sqrt{\frac{(2^\ell-1)}{2}} - (N + 2^n)\varphi_a}{(\lambda N + 2^n)}\right) \\
P_S^{(\mathrm{md,wor,adj})} &= \Phi\left(\frac{N(\lambda-1)\sqrt{\frac{2^\ell-1}{2}} - 2^n\varphi_a}{N(\lambda-1) + 2^n}\right)
\end{aligned}$$

which are identical to the expressions for P_S for sampling with and without replacement as can be obtained from Equation (25) of [7].

7.2 Success Probability for Multiple Linear Cryptanalysis

Let $P_S^{(\mathrm{m,wr},\cdot)}$ denote the success probability of multiple linear cryptanalysis when sampling with replacement is used and let $P_S^{(\mathrm{m,wor},\cdot)}$ denote the success probability of multiple linear cryptanalysis when sampling without replacement is used. The third slot is for the type of key randomisation hypothesis used, i.e., the third slot can be filled up in 4 ways, namely std, adj, radj and wadj. Notice that std, adj, radj and wadj influences only the values of s_0^2 and s_1^2 of (60). Therefore we can get the values of $P_S^{(\mathrm{m,wr},\cdot)}$ and $P_S^{(\mathrm{m,wor},\cdot)}$ by using the corresponding

expressions for σ from (58) and (59) in (60).

$$P_S^{(\mathrm{m,wr},\cdot)} = \Phi\left(\frac{\left(4s_0^2+\frac{1}{N}\right)\left(\ell+\frac{NC^{(\mathrm{m})}}{4Ns_0^2+1}\right)-\left(4s_1^2+\frac{1}{N}\right)\gamma}{\left(4s_0^2+\frac{1}{N}\right)\sqrt{2\left(\ell+\frac{2NC^{(\mathrm{m})}}{4Ns_0^2+1}\right)}}\right); \tag{71}$$

$$P_S^{(\mathrm{m,wor},\cdot)} = \Phi\left(\frac{\left(4s_0^2+\frac{1}{N}\left(1-\frac{N}{2^n}\right)\right)\left(\ell+\frac{NC^{(\mathrm{m})}}{4Ns_0^2+\left(1-\frac{N}{2^n}\right)}\right)-\left(4s_1^2+\frac{1}{N}\left(1-\frac{N}{2^n}\right)\right)\gamma}{\left(4s_0^2+\frac{1}{N}\left(1-\frac{N}{2^n}\right)\right)\sqrt{2\left(\ell+\frac{NC^{(\mathrm{m})}}{4Ns_0^2+\left(1-\frac{N}{2^n}\right)}\right)}}\right). \tag{72}$$

Remarks:

1. If $N \ll 2^n$, then $P_S^{(\mathrm{m,wor},\cdot)} \approx P_S^{(\mathrm{m,wr},\cdot)}$. So, the expression for $P_S^{(\mathrm{m,wor},\cdot)}$ given by (72) becomes useful only when the fraction $N/2^n$ is non-negligible.
2. In the case of sampling with replacement, due to the birthday paradox, having N to be greater than $2^{n/2}$ is not really useful, since repetitions will begin to occur.

7.2.1 Success Probability Under Standard Key Randomisation Hypotheses

Let $P_S^{(\mathrm{m,wr,std})}$ and $P_S^{(\mathrm{m,wor,std})}$ be the success probabilities of multiple linear cryptanalysis for standard multiple right and wrong key randomisation hypotheses corresponding to the situations where plaintexts are chosen with and without replacement respectively. As discussed in Section 4.2, the standard multiple key randomisation hypotheses is obtained from the general multiple key randomisation hypothesis by letting $s_0 \downarrow 0$ and $s_1 \downarrow 0$. Using these conditions in (71) and (72) lead to the following expressions for the success probabilities of multiple linear cryptanalysis in the two cases of sampling with and without replacement.

$$P_S^{(\mathrm{m,wr,std})} = \Phi\left(\frac{\left(\ell+NC^{(\mathrm{m})}\right)-\gamma}{\sqrt{2\left(\ell+2NC^{(\mathrm{m})}\right)}}\right) \tag{73}$$

$$P_S^{(\mathrm{m,wor,std})} = \Phi\left(\frac{\left(\ell+\frac{NC^{(\mathrm{m})}}{\left(1-\frac{N}{2^n}\right)}\right)-\gamma}{\sqrt{2\left(\ell+\frac{NC^{(\mathrm{m})}}{\left(1-\frac{N}{2^n}\right)}\right)}}\right). \tag{74}$$

To the best of our knowledge, no prior work has analysed the success probability of multiple linear cryptanalysis with the standard key randomisation hypotheses and under both the conditions where $P_1, \ldots, P_N$ are chosen uniformly with and without replacement. So, the expressions for $P_S^{(\mathrm{m,wr,std})}$ and $P_S^{(\mathrm{m,wor,std})}$ given by (73) and (74) are the first such results.

7.2.2 Success Probability Under Adjusted Wrong Key Randomisation Hypothesis

Let $P_S^{(\mathrm{m,wr,wadj})}$ and $P_S^{(\mathrm{m,wor,wadj})}$ be the success probabilities of multiple linear cryptanalysis for adjusted wrong key randomisation hypothesis and standard right key randomisation hypothesis corresponding to the situations where plaintexts are chosen with and without replacement respectively.

Setting $s_1^2 = 2^{-n-2}$ converts the general multiple wrong key randomisation hypothesis to the adjusted multiple wrong key randomisation hypothesis. Also, we let $s_0^2 \downarrow 0$, so that the general multiple right key randomisation

hypothesis simplifies to the standard multiple right key randomisation hypothesis. Using the conditions for s_0 and s_1 in (71) and (72) provides the following expressions for the success probabilities in the two cases of sampling with and without replacement.

$$P_S^{(\mathrm{m,wr,wadj})} = \Phi\left(\frac{\left(\ell + NC^{(\mathrm{m})}\right) - \left(1 + \frac{N}{2^n}\right)\gamma}{\sqrt{2\left(\ell + 2NC^{(\mathrm{m})}\right)}}\right); \tag{75}$$

$$P_S^{(\mathrm{m,wor,wadj})} = \Phi\left(\frac{\left(1 - \frac{N}{2^n}\right)\left(\ell + \frac{NC^{(\mathrm{m})}}{\left(1 - \frac{N}{2^n}\right)}\right) - \gamma}{\left(1 - \frac{N}{2^n}\right)\sqrt{2\left(\ell + \frac{NC^{(\mathrm{m})}}{\left(1 - \frac{N}{2^n}\right)}\right)}}\right). \tag{76}$$

To the best of our knowledge, no prior work has analysed the success probability of multiple linear cryptanalysis for the adjusted multiple wrong key randomisation hypothesis and standard multiple right key randomisation hypothesis corresponding to the situation where plaintexts $P_1, \ldots, P_N$ are chosen with and without replacement, respectively. So, the expressions for $P_S^{(\mathrm{m,wr,wadj})}$ and $P_S^{(\mathrm{m,wor,wadj})}$ given by (75) and (76) are the first such results.

7.2.3 Success Probability Under Adjusted Right Key Randomisation Hypothesis

Let $P_S^{(\mathrm{m,wr,radj})}$ and $P_S^{(\mathrm{m,wor,radj})}$ be the success probabilities of multiple linear cryptanalysis for adjusted multiple right key randomisation hypothesis and standard multiple wrong key randomisation hypothesis corresponding to the situations where plaintexts are chosen with and without replacement respectively.

Setting $s_1^2 \downarrow 0$ converts the general multiple wrong key randomisation hypothesis to the standard multiple wrong key randomisation hypothesis. Also, we let $s_0^2 = \sigma^2$, so that the general multiple right key randomisation hypothesis simplifies to the adjusted multiple right key randomisation hypothesis. Using the conditions for s_0 and s_1 in (71) and (72) provides the following expressions for the success probabilities in the two cases of sampling with and without replacement.

$$P_S^{(\mathrm{m,wr,radj})} = \Phi\left(\frac{\left(4N\sigma^2 + 1\right)\left(\ell + \frac{NC^{(\mathrm{m})}}{4N\sigma^2+1}\right) - \gamma}{\left(4N\sigma^2 + 1\right)\sqrt{2\left(\ell + \frac{2NC^{(\mathrm{m})}}{4N\sigma^2+1}\right)}}\right); \tag{77}$$

$$P_S^{(\mathrm{m,wor,radj})} = \Phi\left(\frac{\left(4N\sigma^2 + \left(1 - \frac{N}{2^n}\right)\right)\left(\ell + \frac{NC^{(\mathrm{m})}}{4N\sigma^2+\left(1-\frac{N}{2^n}\right)}\right) - \left(1 - \frac{N}{2^n}\right)\gamma}{\left(4N\sigma^2 + \left(1 - \frac{N}{2^n}\right)\right)\sqrt{2\left(\ell + \frac{NC^{(\mathrm{m})}}{4Ns_0^2+\left(1-\frac{N}{2^n}\right)}\right)}}\right). \tag{78}$$

Remarks: To the best of our knowledge, no prior work has analysed the success probability of multiple linear cryptanalysis with the adjusted right key randomisation hypotheses and under the condition where $P_1, \ldots, P_N$ are chosen uniformly without replacement. So, the expressions for $P_S^{(\mathrm{m,wr,std})}$ and $P_S^{(\mathrm{m,wor,std})}$ given by (77) and (78) are the first such results.

7.2.4 Success Probability Under Adjusted Key Randomisation Hypothesis

Let $P_S^{(\mathrm{m,wr,adj})}$ and $P_S^{(\mathrm{m,wor,adj})}$ be the success probabilities of multiple linear cryptanalysis for both adjusted multiple right and wrong key randomisation hypothesis corresponding to the situations where plaintexts are chosen with and without replacement respectively.

Setting $s_1^2 = 2^{-n-2}$ converts the general multiple wrong key randomisation hypothesis to the adjusted multiple wrong key randomisation hypothesis. Also, we let $s_0^2 = \sigma^2$, so that the general multiple right key randomisation hypothesis simplifies to the standard multiple right key randomisation hypothesis. Using the conditions for s_0 and s_1 in (71) and (72) provides the following expressions for the success probabilities in the two cases of sampling with and without replacement.

$$P_S^{(\mathrm{m,wr,adj})} = \Phi\left(\frac{\left(4N\sigma^2+1\right)\left(\ell+\frac{NC^{(\mathrm{m})}}{4N\sigma^2+1}\right)-\left(1+\frac{N}{2^n}\right)\gamma}{\left(4N\sigma^2+1\right)\sqrt{2\left(\ell+\frac{2NC^{(\mathrm{m})}}{4N\sigma^2+1}\right)}}\right); \tag{79}$$

$$P_S^{(\mathrm{m,wor,adj})} = \Phi\left(\frac{\left(4N\sigma^2+\left(1-\frac{N}{2^n}\right)\right)\left(\ell+\frac{NC^{(\mathrm{m})}}{4N\sigma^2+\left(1-\frac{N}{2^n}\right)}\right)-\gamma}{\left(4N\sigma^2+\left(1-\frac{N}{2^n}\right)\right)\sqrt{2\left(\ell+\frac{NC^{(\mathrm{m})}}{4N\sigma^2+\left(1-\frac{N}{2^n}\right)}\right)}}\right). \tag{80}$$

Expressions for the success probability of multiple linear cryptanalysis under adjusted multiple right and wrong key randomisation hypotheses corresponding to sampling with and without repetitions were obtained in [7]. These expressions were obtained for large values of ℓ. The validity condition of $\ell > 50$ was mentioned in [7]. This condition arises due to the requirement of approximating the central chi-squared distribution by a normal distribution. Following [7], assume that $C^{(\mathrm{m})} = 0$, $C = \frac{\lambda\ell}{2^n}$ and $\lambda \geq 1$. To approximate the central chi-square distribution by a normal distribution as in [7] it is required to replace γ by $(2^\ell - 1) + \sqrt{2(2^\ell - 1)}\varphi_a$. Proceeding as in Section 7.1.4, it can be shown that the resulting expressions for P_S that are obtained are identical to the expressions of P_S for both sampling with and without replacement as can be obtained from Equation (25) of [7].

8 Dependence of P_S on N

We have obtained various expressions for the success probability in terms of the data complexity N and the advantage a. For a fixed value of a, it is perhaps intuitive that the success probability is a monotone increasing function of N. On the other hand, the nature of the expressions for P_S shows a complicated dependence on N. It is of interest to exactly characterise the conditions under which P_S indeed increases monotonically with N. We perform this task in the present section.

8.1 Multidimensional Case

Consider the general expression for the success probability P_S as given by (56). The subsequent expressions for success probability with/without replacement and under different possible combinations of standard/adjusted multidimensional key randomisation hypotheses are all obtained as special cases of (56). In (56), the quantities s_0, s_1 and γ are constants which are independent of N and only σ and $\delta_{(\mathrm{md})}$ depends on N as shown in (54) and (55). Further, from (54) and (55), it is clear that σ is a decreasing function of N for both the cases of with and without replacements, whereas $\delta_{(\mathrm{md})}$ is an increasing function in both cases.

We analyse the behaviour of P_S as a function of N and identify the situations where P_S is a monotonic increasing function of N.

Theorem 4. *Consider P_S to be given by (56) where s_0, s_1 and γ are positive and independent of N while $\sigma > 0$ is a monotone decreasing function of N and $\delta_{(\mathrm{md})}$ is a monotone increasing function of N.*

1. *Suppose $s_0^2 \geq s_1^2$. Then P_S is an increasing function of N for all $N > 0$.*

2. Suppose $s_0 < s_1$. Then P_S is a decreasing function of N if and only if

$$C^{(\mathrm{md})} < \sqrt{\gamma\left(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})}\right)\left[\gamma\left(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})}\right) + 2^{\ell+1}(2^\ell - 1)(s_1^2 - s_0^2)\right]} - \gamma\left(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})}\right).$$

Proof. We proceed by taking derivatives with respect to N. Since σ is a decreasing function of N, $\frac{d\sigma^2_{(\mathrm{md})}}{dN} < 0$. Similarly, as $\delta_{(\mathrm{md})}$ is an increasing function of N, $\frac{d\delta_{(\mathrm{md})}}{dN} > 0$.

$$\begin{aligned}
\frac{dP_S}{dN} &= \phi\left(\frac{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})((2^\ell - 1) + \delta_{(\mathrm{md})}) - (2^\ell s_1^2 + \sigma^2_{(\mathrm{md})})\gamma}{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})\sqrt{2((2^\ell - 1) + 2\delta_{(\mathrm{md})})}}\right) \times \\
&\quad \left[\frac{((2^\ell - 1) + \delta_{(\mathrm{md})})\frac{d\sigma^2_{(\mathrm{md})}}{dN} + (2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})\frac{d\delta_{(\mathrm{md})}}{dN} - \gamma\frac{d\sigma^2_{(\mathrm{md})}}{dN}}{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})\sqrt{2((2^\ell - 1) + 2\delta_{(\mathrm{md})})}} - \left\{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})((2^\ell - 1) + \delta_{(\mathrm{md})}) - \right.\right. \\
&\quad \left.\left.(2^\ell s_1^2 + \sigma^2_{(\mathrm{md})})\gamma\right\}\frac{\left\{\sqrt{2((2^\ell - 1) + 2\delta_{(\mathrm{md})})}\frac{d\sigma^2_{(\mathrm{md})}}{dN} + \frac{2(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})}{\sqrt{2((2^\ell - 1) + 2\delta_{(\mathrm{md})})}}\frac{d\delta_{(\mathrm{md})}}{dN}\right\}}{\left\{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})\sqrt{2((2^\ell - 1) + 2\delta_{(\mathrm{md})})}\right\}^2}\right] \\
&= \phi\left(\frac{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})((2^\ell - 1) + \delta_{(\mathrm{md})}) - (2^\ell s_1^2 + \sigma^2_{(\mathrm{md})})\gamma}{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})\sqrt{2((2^\ell - 1) + 2\delta_{(\mathrm{md})})}}\right) \times \\
&\quad \left[\frac{((2^\ell - 1) + \delta_{(\mathrm{md})} - \gamma)\frac{d\sigma^2_{(\mathrm{md})}}{dN} + (2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})\frac{d\delta_{(\mathrm{md})}}{dN}}{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})\sqrt{2((2^\ell - 1) + 2\delta_{(\mathrm{md})})}} - \left\{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})((2^\ell - 1) + \delta_{(\mathrm{md})}) - \right.\right. \\
&\quad \left.\left.(2^\ell s_1^2 + \sigma^2_{(\mathrm{md})})\gamma\right\}\frac{\left\{\left(2((2^\ell - 1) + 2\delta_{(\mathrm{md})})\right)\frac{d\sigma^2_{(\mathrm{md})}}{dN} + 2(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})\frac{d\delta_{(\mathrm{md})}}{dN}\right\}}{\left\{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})\sqrt{2((2^\ell - 1) + 2\delta_{(\mathrm{md})})}\right\}^2\sqrt{2((2^\ell - 1) + 2\delta_{(\mathrm{md})})}}\right] \\
&= \frac{\phi\left(\frac{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})((2^\ell - 1) + \delta_{(\mathrm{md})}) - (2^\ell s_1^2 + \sigma^2_{(\mathrm{md})})\gamma}{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})\sqrt{2((2^\ell - 1) + 2\delta_{(\mathrm{md})})}}\right)}{\left\{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})\sqrt{2((2^\ell - 1) + 2\delta_{(\mathrm{md})})}\right\}^2\sqrt{2((2^\ell - 1) + 2\delta_{(\mathrm{md})})}} \\
&\quad \left[\left\{((2^\ell - 1) + \delta_{(\mathrm{md})} - \gamma)\frac{d\sigma^2_{(\mathrm{md})}}{dN} + (2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})\frac{d\delta_{(\mathrm{md})}}{dN}\right\}\left\{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})\left(2((2^\ell - 1) + 2\delta_{(\mathrm{md})})\right)\right\} - \right. \\
&\quad \left\{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})((2^\ell - 1) + \delta_{(\mathrm{md})}) - (2^\ell s_1^2 + \sigma^2_{(\mathrm{md})})\gamma\right\} \times \\
&\quad \left.\left\{\left(2((2^\ell - 1) + 2\delta_{(\mathrm{md})})\right)\frac{d\sigma^2_{(\mathrm{md})}}{dN} + 2(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})\frac{d\delta_{(\mathrm{md})}}{dN}\right\}\right].
\end{aligned}$$

Now,

$$\frac{\phi\left(\frac{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})((2^\ell - 1) + \delta_{(\mathrm{md})}) - (2^\ell s_1^2 + \sigma^2_{(\mathrm{md})})\gamma}{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})\sqrt{2((2^\ell - 1) + 2\delta_{(\mathrm{md})})}}\right)}{\left\{(2^\ell s_0^2 + \sigma^2_{(\mathrm{md})})\sqrt{2((2^\ell - 1) + 2\delta_{(\mathrm{md})})}\right\}^2\sqrt{2((2^\ell - 1) + 2\delta_{(\mathrm{md})})}} > 0.$$

This implies that $\frac{dP_S}{dN} > 0$ if and only if $g(N) > 0$ where

$$\begin{aligned}
g(N) &= \left\{((2^\ell - 1) + \delta_{(\text{md})} - \gamma)\frac{d\sigma^2_{(\text{md})}}{dN} + (2^\ell s_0^2 + \sigma^2_{(\text{md})})\frac{d\delta_{(\text{md})}}{dN}\right\}\left\{(2^\ell s_0^2 + \sigma^2_{(\text{md})})\left(2((2^\ell - 1) + 2\delta_{(\text{md})})\right)\right\} - \\
&\quad \left\{(2^\ell s_0^2 + \sigma^2_{(\text{md})})((2^\ell - 1) + \delta_{(\text{md})}) - (2^\ell s_1^2 + \sigma^2_{(\text{md})})\gamma\right\}\left\{\left(2((2^\ell - 1) + 2\delta_{(\text{md})})\right)\frac{d\sigma^2_{(\text{md})}}{dN} + \right. \\
&\quad \left. 2(2^\ell s_0^2 + \sigma^2_{(\text{md})})\frac{d\delta_{(\text{md})}}{dN}\right\} \\
&= \left\{\left\{((2^\ell - 1) + \delta_{(\text{md})} - \gamma)\right\}\left\{(2^\ell s_0^2 + \sigma^2_{(\text{md})})\left(2((2^\ell - 1) + 2\delta_{(\text{md})})\right)\right\} - \right. \\
&\quad \left.\left\{(2^\ell s_0^2 + \sigma^2_{(\text{md})})((2^\ell - 1) + \delta_{(\text{md})}) - (2^\ell s_1^2 + \sigma^2_{(\text{md})})\gamma\right\}\left\{\left(2((2^\ell - 1) + 2\delta_{(\text{md})})\right)\right\}\right\}\frac{d\sigma^2_{(\text{md})}}{dN} + \\
&\quad \left\{\left\{(2^\ell s_0^2 + \sigma^2_{(\text{md})})\right\}\left\{2(2^\ell s_0^2 + \sigma^2_{(\text{md})})\left((2^\ell - 1) + \delta_{(\text{md})}\right) + 2(2^\ell s_0^2 + \sigma^2_{(\text{md})})\delta_{(\text{md})}\right\} - \right. \\
&\quad \left.\left\{(2^\ell s_0^2 + \sigma^2_{(\text{md})})((2^\ell - 1) + \delta_{(\text{md})}) - (2^\ell s_1^2 + \sigma^2_{(\text{md})})\gamma\right\}\left\{2(2^\ell s_0^2 + \sigma^2_{(\text{md})})\right\}\right\}\frac{d\delta_{(\text{md})}}{dN} \\
&= 2^\ell\gamma(s_1^2 - s_0^2)\left(2((2^\ell - 1) + 2\delta_{(\text{md})})\right)\frac{d\sigma^2_{(\text{md})}}{dN} + 2(2^\ell s_0^2 + \sigma^2_{(\text{md})}) \times \\
&\quad \left\{(2^\ell s_0^2 + \sigma^2_{(\text{md})})\delta_{(\text{md})} + (2^\ell s_1^2 + \sigma^2_{(\text{md})})\gamma\right\}\frac{d\delta_{(\text{md})}}{dN}.
\end{aligned}$$

Case $s_0^2 \geq s_1^2$: Since $s_1^2 - s_0^2 \leq 0$, $2^\ell\gamma\left(2((2^\ell - 1) + 2\delta_{(\text{md})})\right) > 0$ and $\frac{d\sigma^2_{(\text{md})}}{dN} < 0$, therefore

$$2^\ell\gamma(s_1^2 - s_0^2)\left(2((2^\ell - 1) + 2\delta_{(\text{md})})\right)\frac{d\sigma^2_{(\text{md})}}{dN} > 0.$$

Similarly, as $\frac{d\delta_{(\text{md})}}{dN} > 0$ and $2(2^\ell s_0^2 + \sigma^2_{(\text{md})})\left\{(2^\ell s_0^2 + \sigma^2_{(\text{md})})\delta_{(\text{md})} + (2^\ell s_1^2 + \sigma^2_{(\text{md})})\gamma\right\} > 0$, we have

$$2(2^\ell s_0^2 + \sigma^2_{(\text{md})})\left\{(2^\ell s_0^2 + \sigma^2_{(\text{md})})\delta_{(\text{md})} + (2^\ell s_1^2 + \sigma^2_{(\text{md})})\gamma\right\}\frac{d\delta_{(\text{md})}}{dN} > 0.$$

So, $g(N) > 0$ for all N and consequently, $\frac{dP_S}{dN} > 0$ for all N implying that P_S is a strictly increasing function of N.

Case $s_0^2 < s_1^2$: From (54) and (55), we can write

$$\delta_{(\text{md})} = \frac{C^{(\text{md})}}{A + B + \sigma^2_{(\text{md})}}, \tag{81}$$

where

$$A = \begin{cases} 0; & \text{for sampling with replacement;} \\ 2^{-\ell}(1 - 2^\ell); & \text{for sampling without replacement,} \end{cases}$$

and

$$B = \begin{cases} 2^\ell s_0^2; & \text{for sampling with replacement;} \\ 2^\ell s_0^2 - 2^{-\ell}(1 - 2^\ell); & \text{for sampling without replacement.} \end{cases}$$

$$\frac{d\delta_{(\mathrm{md})}}{dN} = -\frac{C^{(\mathrm{md})}}{\{A+B+\sigma^2_{(\mathrm{md})}\}^2}\frac{d\sigma^2_{(\mathrm{md})}}{dN} = -\frac{\delta^2_{(\mathrm{md})}}{C^{(\mathrm{md})}}\cdot\frac{d\sigma^2_{(\mathrm{md})}}{dN}.$$

Therefore,

$$\begin{aligned} g(N) &= 2^\ell\gamma(s_1^2-s_0^2)\left(2((2^\ell-1)+2\delta_{(\mathrm{md})})\right)\frac{d\sigma^2_{(\mathrm{md})}}{dN} - 2(2^\ell s_0^2+\sigma^2_{(\mathrm{md})})\times \\ &\quad \frac{\left\{(2^\ell s_0^2+\sigma^2_{(\mathrm{md})})\delta_{(\mathrm{md})}+(2^\ell s_1^2+\sigma^2_{(\mathrm{md})})\gamma\right\}\delta^2_{(\mathrm{md})}}{C^{(\mathrm{md})}}\frac{d\sigma^2_{(\mathrm{md})}}{dN} \\ &= \frac{f(N)}{C^{(\mathrm{md})}}\frac{d\sigma^2_{(\mathrm{md})}}{dN} \text{ (say)}, \end{aligned}$$

where,

$$\begin{aligned} f(N) &= 2^\ell\gamma(s_1^2-s_0^2)\left(2((2^\ell-1)+2\delta_{(\mathrm{md})})\right)C^{(\mathrm{md})} - 2(2^\ell s_0^2+\sigma^2_{(\mathrm{md})})\times \\ &\quad \left\{(2^\ell s_0^2+\sigma^2_{(\mathrm{md})})\delta_{(\mathrm{md})}+(2^\ell s_1^2+\sigma^2_{(\mathrm{md})})\gamma\right\}\delta^2_{(\mathrm{md})}. \end{aligned}$$

In this case P_S is decreasing if and only if $f(N)>0$.

Let us simplify the expression of $f(N)$ to get a condition on $C^{(\mathrm{md})}$. Assume

$$\zeta = 2^\ell s_0^2+\sigma^2_{(\mathrm{md})} \quad \text{and} \quad \xi = 2^\ell s_1^2+\sigma^2_{(\mathrm{md})}.$$

Then,

$$\begin{aligned} f(N) &= \gamma(\xi-\zeta)\left(2((2^\ell-1)+2\delta_{(\mathrm{md})})\right)C^{(\mathrm{md})} - 2\zeta\left\{\zeta\delta_{(\mathrm{md})}+\xi\gamma\right\}\delta^2_{(\mathrm{md})} \\ &= \gamma(\xi-\zeta)\left(2((2^\ell-1)+2\delta_{(\mathrm{md})})\right)\delta_{(\mathrm{md})}\left(A+B+\sigma^2_{(\mathrm{md})}\right) - 2\zeta\left\{\zeta\delta_{(\mathrm{md})}+\xi\gamma\right\}\delta^2_{(\mathrm{md})} \\ &= 2\delta_{(\mathrm{md})}\left[\gamma(\xi-\zeta)((2^\ell-1)+2\delta_{(\mathrm{md})})\left(A+B+\sigma^2_{(\mathrm{md})}\right) - 2\zeta\left\{\zeta\delta_{(\mathrm{md})}+\xi\gamma\right\}\delta_{(\mathrm{md})}\right] \\ &= 2\delta_{(\mathrm{md})}\left[\gamma(\xi-\zeta)(2^\ell-1)\left(A+B+\sigma^2_{(\mathrm{md})}\right)+2\gamma(\xi-\zeta)\left(A+B+\sigma^2_{(\mathrm{md})}\right)\delta_{(\mathrm{md})} - 2\zeta^2\delta^2_{(\mathrm{md})} - \right. \\ &\quad \left. 2\zeta\xi\gamma\delta_{(\mathrm{md})}\right] \\ &= -2\delta_{(\mathrm{md})}\left[2\zeta^2\delta^2_{(\mathrm{md})} - 2\gamma\left\{(\xi-\zeta)\left(A+B+\sigma^2_{(\mathrm{md})}\right)-\zeta\xi\right\}\delta_{(\mathrm{md})} - \gamma(\xi-\zeta)(2^\ell-1)\left(A+B+\sigma^2_{(\mathrm{md})}\right)\right]. \end{aligned}$$

Since, $-2\delta_{(\mathrm{md})}<0$, therefore $f(N)>0$ if and only if

$$2\zeta^2\delta^2_{(\mathrm{md})} - 2\gamma\left\{(\xi-\zeta)\left(A+B+\sigma^2_{(\mathrm{md})}\right)-\zeta\xi\right\}\delta_{(\mathrm{md})} - \gamma(\xi-\zeta)(2^\ell-1)\left(A+B+\sigma^2_{(\mathrm{md})}\right)<0. \tag{82}$$

The discriminant of the quadratic equation in $\delta_{(\mathrm{md})}$ is given by

$$4\Delta^2 = 4\left[\gamma^2\left\{(\xi-\zeta)\left(A+B+\sigma^2_{(\mathrm{md})}\right)-\zeta\xi\right\}^2 + 2\gamma\zeta^2(\xi-\zeta)(2^\ell-1)\left(A+B+\sigma^2_{(\mathrm{md})}\right)\right]>0.$$

Therefore, both the roots of the quadratic is real. Let $r_1<r_2$ be the two roots of the above quadratic equation.

Then (82) holds if and only if $r_1 < \delta_{(\mathrm{md})} < r_2$, where

$$\begin{aligned} r_1 &= \frac{\gamma\left\{(\xi-\zeta)\left(A+B+\sigma^2_{(\mathrm{md})}\right)-\zeta\xi\right\}-\Delta}{\zeta^2} \\ &= \frac{\gamma\left\{2^\ell(s_1^2-s_0^2)\left(A+B+\sigma^2_{(\mathrm{md})}\right)-(2^\ell s_0^2+\sigma^2_{(\mathrm{md})})(2^\ell s_1^2+\sigma^2_{(\mathrm{md})})\right\}-\Delta}{(2^\ell s_0^2+\sigma^2_{(\mathrm{md})})^2} \text{ and} \\ r_2 &= \frac{\gamma\left\{2^\ell(s_1^2-s_0^2)\left(A+B+\sigma^2_{(\mathrm{md})}\right)-(2^\ell s_0^2+\sigma^2_{(\mathrm{md})})(2^\ell s_1^2+\sigma^2_{(\mathrm{md})})\right\}+\Delta}{(2^\ell s_0^2+\sigma^2_{(\mathrm{md})})^2}. \end{aligned}$$

For both sampling with and without replacement we have $A+B+\sigma^2_{(\mathrm{md})} = 2^\ell s_0^2+\sigma^2_{(\mathrm{md})}$. Therefore we have,

$$\begin{aligned} \Delta^2 &= \left[\gamma^2\left\{2^\ell(s_1^2-s_0^2)\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right)-\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right)\left(2^\ell s_1^2+\sigma^2_{(\mathrm{md})}\right)\right\}^2+\right. \\ &\quad \left. 2\gamma\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right)^2 2^\ell(s_1^2-s_0^2)(2^\ell-1)\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right)\right] \\ &= \gamma\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right)^3\left[\gamma\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right)+2^{\ell+1}(2^\ell-1)(s_1^2-s_0^2)\right] \\ r_1 &= -\frac{\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right)\sqrt{\gamma\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right)\left[\gamma\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right)+2^{\ell+1}(2^\ell-1)(s_1^2-s_0^2)\right]}+\gamma\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right)^2}{(2^\ell s_0^2+\sigma^2_{(\mathrm{md})})^2} \\ &= -\frac{\sqrt{\gamma\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right)\left[\gamma\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right)+2^{\ell+1}(2^\ell-1)(s_1^2-s_0^2)\right]}+\gamma\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right)}{(2^\ell s_0^2+\sigma^2_{(\mathrm{md})})} \text{ and} \\ r_2 &= \frac{\sqrt{\gamma\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right)\left[\gamma\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right)+2^{\ell+1}(2^\ell-1)(s_1^2-s_0^2)\right]}-\gamma\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right)}{(2^\ell s_0^2+\sigma^2_{(\mathrm{md})})} \end{aligned}$$

Using (81), $r_1 < \delta_{(\mathrm{md})} < r_2$, $r_1 < 0$ and $C^{(\mathrm{md})} > 0$, we obtain

$$r_1 < \frac{C^{(\mathrm{md})}}{2^\ell s_0^2+\sigma^2_{(\mathrm{md})}} < r_2 \quad \Leftrightarrow \quad 0 < C^{(\mathrm{md})} < r_2(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}).$$

Therefore, P_S is a decreasing function if and only if $f(N) > 0$ if and only if $C^{(\mathrm{md})} < r_2$, i.e.,

$$C^{(\mathrm{md})} < \sqrt{\gamma\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right)\left[\gamma\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right)+2^{\ell+1}(2^\ell-1)(s_1^2-s_0^2)\right]}-\gamma\left(2^\ell s_0^2+\sigma^2_{(\mathrm{md})}\right).$$

□

Under Standard Multidimensional Key Randomisation Hypotheses: In this scenario, both $s_1 = s_0 = 0$. By Condition 1 of Theorem 4, both $P_S^{(\mathrm{md,wr,std})}$ and $P_S^{(\mathrm{md,wor,std})}$ are increasing functions of N.

Under Adjusted Multidimensional Wrong Key Randomisation Hypotheses: In this scenario, $s_1^2 = \frac{1}{2^{n+\ell}}\left(1-\frac{1}{2^\ell}\right)$ and $s_0 = 0$. By Condition 2 of Theorem 4, both $P_S^{(\mathrm{md,wr,wadj})}$ and $P_S^{(\mathrm{md,wor,wadj})}$ are monotonic decreasing functions of N if and only if

$$C^{(\mathrm{md})} < \sqrt{\gamma\left\{\gamma\sigma_{(\mathrm{md})}^2 + \frac{(2^\ell-1)^2}{2^{n+\ell-1}}\right\}} - \gamma\sigma.$$

Under Adjusted Multidimensional Right Key Randomisation Hypotheses: In this scenario, $s_1 = 0$ and $s_0^2 = \frac{C - C^{(\mathrm{md})}}{2^{2\ell}}$. By Condition 1 of Theorem 4, both $P_S^{(\mathrm{md,wr,radj})}$ and $P_S^{(\mathrm{md,wor,radj})}$ are increasing functions of N.

Under Adjusted Multidimensional Key Randomisation Hypotheses: In this scenario, $s_1^2 = \frac{1}{2^{n+\ell}}\left(1-\frac{1}{2^\ell}\right)$ and $s_0^2 = \frac{C - C^{(\mathrm{md})}}{2^{2\ell}}$. By Condition 2 of Theorem 4, both $P_S^{(\mathrm{md,wr,adj})}$ and $P_S^{(\mathrm{md,wor,adj})}$ are monotonic decreasing functions of N if and only if $s_1 > s_0$ and

$$C^{(\mathrm{md})} < \sqrt{\gamma\left(s_0^2+\sigma_{(\mathrm{md})}^2\right)\left[\gamma\left(s_0^2+\sigma_{(\mathrm{md})}^2\right) + 2(2^\ell-1)\left(\frac{1}{2^n}\left(1-\frac{1}{2^\ell}\right) - s_0^2\right)\right]} - \gamma\left(s_0^2+\sigma_{(\mathrm{md})}^2\right).$$

8.2 Multiple Case

Consider the general expression for the success probability P_S in the multiple case, as given by (60). The subsequent expressions for success probability with/without replacement and under standard/adjusted multiple key randomisation hypotheses are all obtained as special cases of (60). In (60), the quantities s_0, s_1 and γ are constants which are independent of N and only σ and $\delta_{(\mathrm{m})}$ depends on N as shown in (58) and (59). Further, from (58) and (59), it is clear that $\sigma_{(\mathrm{m})}^2$ is a decreasing function of N for both the cases of sampling with and without replacements, whereas $\delta_{(\mathrm{m})}$ is an increasing function in both cases.

Theorem 5. *Consider P_S to be given by (60) where s_0, s_1 and γ are positive and independent of N while $\sigma > 0$ is a monotone decreasing function of N and $\delta_{(\mathrm{m})}$ is a monotone increasing function of N.*

1. *Suppose $s_0^2 \geq s_1^2$. Then P_S is an increasing function of N for all $N > 0$.*
2. *Suppose $s_0 < s_1$. Then P_S is a decreasing function of N if and only if*

$$C^{(\mathrm{m})} < \sqrt{\gamma\left(4s_0^2+\sigma_{(\mathrm{m})}^2\right)\left[\gamma\left(4s_0^2+\sigma_{(\mathrm{m})}^2\right) + 8\ell\left(s_1^2-s_0^2\right)\right]} - \gamma\left(4s_0^2+\sigma_{(\mathrm{m})}^2\right).$$

Proof. The proof is similar to the proof of Theorem 4. The expression for P_S in the case of multiple linear cryptanalysis is given by (60) while that of multidimensional linear cryptanalysis is given by (56). In (56), first replace $2^\ell s_0^2$, $2^\ell s_1^2$ and $(2^\ell - 1) + 2\delta$ by $\Lambda_1 s_0^2$, $\Lambda_1 s_1^2$ and $\Lambda_2 + 2\delta$ respectively and then replace $\Lambda_1 s_0^2$, $\Lambda_1 s_1^2$ and $\Lambda_2 + 2\delta$ by $4s_0^2$, $4s_1^2$ and $\ell + 2\delta$ respectively to obtain (60). This shows the similarity between the expressions for P_S given by (60) and (56). Using this similarity, it is possible to do the computations as in the proof of Theorem 4 to obtain the desired result. □

Under Standard Multiple Key Randomisation Hypotheses: In this scenario, both $s_1 = s_0 = 0$. By Condition 1 of Theorem 5, both $P_S^{(\mathrm{m,wr,std})}$ and $P_S^{(\mathrm{m,wor,std})}$ are increasing functions of N.

Under Adjusted Multiple Wrong Key Randomisation Hypotheses: In this scenario, $s_1^2 = 2^{-n-2}$ and $s_0 = 0$. By Condition 2 of Theorem 5, both $P_S^{(\mathrm{m,wr,wadj})}$ and $P_S^{(\mathrm{m,wor,wadj})}$ are monotonic decreasing functions of N if and only if

$$C^{(\mathrm{m})} < \sqrt{\gamma\sigma_{(\mathrm{m})}^2 \left\{\gamma\sigma_{(\mathrm{m})}^2 + 2^{-(n-1)}\ell\right\}} - \gamma\sigma_{(\mathrm{m})}^2$$

Under Adjusted Multiple Right Key Randomisation Hypotheses: In this scenario, $s_1 = 0$ and $s_0^2 > 0$. By Condition 1 of Theorem 5, both $P_S^{(\mathrm{m,wr,radj})}$ and $P_S^{(\mathrm{m,wor,radj})}$ are increasing functions of N.

Under Adjusted Multiple Key Randomisation Hypotheses: In this scenario, $s_1^2 = 2^{-n-2}$ and $s_0^2 > 0$. By Condition 2 of Theorem 5, both $P_S^{(\mathrm{m,wr,adj})}$ and $P_S^{(\mathrm{m,wor,adj})}$ are monotonic decreasing functions of N if and only if $s_1 > s_0$ and

$$C^{(\mathrm{m})} < \sqrt{\gamma\left(4s_0^2 + \sigma_{(\mathrm{m})}^2\right)\left[\gamma\left(4s_0^2 + \sigma_{(\mathrm{m})}^2\right) + 8\ell\left(2^{-n-2} - s_0^2\right)\right]} - \gamma\left(4s_0^2 + \sigma_{(\mathrm{m})}^2\right).$$

9 Conclusion

This work introduced the general key randomisation hypotheses and the standard/adjusted key randomisation hypotheses can be obtained as special cases. Expressions for the success probabilities under the different settings of multidimensional/multiple and sampling with/without replacement have been obtained. The dependence of the success probability on the data complexity have been completely characterised. The statistical analysis has been rigorous to the extent possible. Certain heuristic assumptions seem to be inherently unavoidable; these have been identified and the difficulties in avoiding these heuristics have been carefully explained. We believe that the current work provides a deeper understanding of statistical analysis of attack using several linear approximations than what was previously known.

References

[1] Tomer Ashur, Tim Beyne, and Vincent Rijmen. Revisiting the wrong-key-randomization hypothesis. *IACR Cryptology ePrint Archive*, 2016:990, 2016.

[2] Thomas Baignères, Pascal Junod, and Serge Vaudenay. How Far Can We Go Beyond Linear Cryptanalysis? In *Advances in Cryptology–ASIACRYPT 2004*, pages 432–450. Springer, 2004.

[3] Thomas Baignères, Pouyan Sepehrdad, and Serge Vaudenay. Distinguishing Distributions Using Chernoff Information. In *Provable Security*, pages 144–165. Springer, 2010.

[4] Alex Biryukov, Christophe De Cannière, and Michaël Quisquater. On Multiple Linear Approximations. In *Advances in Cryptology–CRYPTO 2004*, pages 1–22. Springer, 2004.

[5] Céline Blondeau, Benoît Gérard, and Kaisa Nyberg. Multiple Differential Cryptanalysis using LLR and χ^2 Statistics. In *Security and Cryptography for Networks*, pages 343–360. Springer, 2012.

[6] Céline Blondeau and Kaisa Nyberg. Joint Data and Key Distribution of the Linear Cryptanalysis Test Statistic and Its Impact to Data Complexity Estimates of Multiple/Multidimensional Linear and Truncated Differential Attacks, version dated 24 september, 2015. *IACR Cryptology ePrint Archive*, 2015:935, 2015. `http://eprint.iacr.org/2015/935`.

[7] Céline Blondeau and Kaisa Nyberg. Joint data and key distribution of simple, multiple, and multidimensional linear cryptanalysis test statistic and its impact to data complexity. *Des. Codes Cryptography*, 82(1-2):319–349, 2017.

[8] Andrey Bogdanov, Huizheng Geng, Meiqin Wang, Long Wen, and Baudoin Collard. Zero-correlation linear cryptanalysis with FFT and improved attacks on ISO standards camellia and CLEFIA. In Tanja Lange, Kristin E. Lauter, and Petr Lisonek, editors, *Selected Areas in Cryptography - SAC 2013 - 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers*, volume 8282 of *Lecture Notes in Computer Science*, pages 306–323. Springer, 2013.

[9] Andrey Bogdanov, Gregor Leander, Kaisa Nyberg, and Meiqin Wang. Integral and multidimensional linear distinguishers with correlation zero. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, volume 7658 of *Lecture Notes in Computer Science*, pages 244–261. Springer, 2012.

[10] Andrey Bogdanov and Vincent Rijmen. Linear hulls with correlation zero and linear cryptanalysis of block ciphers. *Des. Codes Cryptography*, 70(3):369–383, 2014.

[11] Andrey Bogdanov and Elmar Tischhauser. On the Wrong Key Randomisation and Key Equivalence Hypotheses in Matsui's Algorithm 2. In *Fast Software Encryption*, pages 19–38. Springer, 2014.

[12] Andrey Bogdanov and Meiqin Wang. Zero correlation linear cryptanalysis with reduced data complexity. In *Fast Software Encryption*, pages 29–48. Springer, 2012.

[13] Joan Daemen and Vincent Rijmen. Probability Distributions of Correlation and Differentials in Block Ciphers. *IACR Cryptology ePrint Archive*, 2005:212, 2005. `http://eprint.iacr.org/2005/212`.

[14] Joan Daemen and Vincent Rijmen. Probability Distributions of Correlation and Differentials in Block Ciphers. *Journal of Mathematical Cryptology JMC*, 1(3):221–242, 2007.

[15] Carlo Harpes, Gerhard G. Kramer, and James L. Massey. A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-Up Lemma. In *Advances in Cryptology - EUROCRYPT '95, International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 21-25, 1995, Proceeding*, pages 24–38, 1995. `http://link.springer.de/link/service/series/0558/bibs/0921/09210024.htm`.

[16] Miia Hermelin, Joo Yeon Cho, and Kaisa Nyberg. Multidimensional Extension of Matsui's Algorithm 2. In *Fast Software Encryption*, pages 209–227. Springer, 2009.

[17] Jialin Huang, Serge Vaudenay, Xuejia Lai, and Kaisa Nyberg. Capacity and Data Complexity in Multidimensional Linear Attack. In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, pages 141–160, 2015. `http://dx.doi.org/10.1007/978-3-662-47989-6_7`.

[18] Norman Lloyd Johnson, Samuel Kotz, and Narayanaswamy Balakrishnan. *Continuous Univariate Distributions, Volume 2*. Wiley Series in Probability and Statistics. John Wiley & Sons, second edition, 1995.

[19] Pascal Junod. On the Optimality of Linear, Differential, and Sequential Distinguishers. In *Advances in Cryptology–EUROCRYPT 2003*, pages 17–32. Springer, 2003.

[20] Burton S Kaliski Jr and Matthew JB Robshaw. Linear Cryptanalysis Using Multiple Approximations. In *Advances in Cryptology–Crypto'94*, pages 26–39. Springer, 1994.

[21] Mitsuru Matsui. Linear Cryptanalysis Method for DES Cipher. In *Advances in Cryptology–EUROCRYPT'93*, pages 386–397. Springer, 1993.

[22] Mitsuru Matsui. The First Experimental Cryptanalysis of the Data Encryption Standard. In Y. G. Desmedt, editor, *Advances in Cryptology–Crypto'94*, pages 1–11. Springer, 1994.

[23] Sean Murphy. The Independence of Linear Approximations in Symmetric Cryptanalysis. *IEEE Transactions on Information Theory*, 52(12):5510–5518, 2006.

[24] Subhabrata Samajder and Palash Sarkar. Rigorous upper bounds on data complexities of block cipher cryptanalysis. *IACR Cryptology ePrint Archive*, 2015:916, 2015.

[25] Subhabrata Samajder and Palash Sarkar. Another look at normal approximations in cryptanalysis. *J. Mathematical Cryptology*, 10(2):69–99, 2016.

[26] Subhabrata Samajder and Palash Sarkar. A new test statistic for key recovery attacks using multiple linear approximations. In *Mycrypt 2016*, volume 10311 of *LNCS*, pages 277–293. Springer, 2016.

[27] Subhabrata Samajder and Palash Sarkar. Another look at success probability in linear cryptanalysis. Cryptology ePrint Archive, Report 2017/391, 2017. `http://eprint.iacr.org/2017/391`.

[28] Ali Aydın Selçuk. On Probability of Success in Linear and Differential Cryptanalysis. *Journal of Cryptology*, 21(1):131–147, 2008.

[29] Robert J Serfling. *Approximation Theorems of Mathematical Statistics*, volume 162. John Wiley & Sons, 2009.

[30] Anne Tardy-Corfdir and Henri Gilbert. A Known Plaintext Attack of FEAL-4 and FEAL-6. In Joan Feigenbaum, editor, *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings*, volume 576 of *Lecture Notes in Computer Science*, pages 172–181. Springer, 1991.

[31] A. M. Walker. A Note on the Asymptotic Distribution of Sample Quantiles. *Journal of the Royal Statistical Society. Series B (Methodological)*, 30(3):pp. 570–575, 1968.

A Some Results on Statistics

A.1 Multivariate Normal to Chi-square

This section looks at certain conditions under which XX^t follows a (possibly non-central) chi-square distribution, where X follows a multivariate normal distribution with singular variance-covariance matrix. The result can be found in [29, Chapter 3.5].

Theorem 6. *Let $X = (X_1, \ldots, X_\tau)$ be $\mathcal{N}(\mu, \Sigma)$, and let $B_{\tau\times\tau}$ be a symmetric matrix. Assume that, for $\eta = (\eta_1, \ldots, \eta_\tau)$,*

$$\eta\Sigma = 0 \Rightarrow \eta\mu^t = 0,$$

where the superscript t denotes the transpose of a matrix. The XBX^t has a (possibly non-central) chi-square distribution if and only if

$$\Sigma B\Sigma B\Sigma = \Sigma B\Sigma,$$

in which case the degrees of freedom if trace $(B\Sigma)$ and the non-centrality parameter is $\mu B\mu^t$.

From the above theorem we can now lists the following assumptions under which XX^t follows a (possibly non-central) chi-square distribution with $(\tau - 1)$ degrees of freedom, where X follows a multivariate normal distribution with singular variance-covariance matrix.

1. There exists an η such that
$$\eta\Sigma = 0 \Rightarrow \eta\mu^t = 0.$$
2. Here $B = I_\tau$.
3. $\Sigma^2 = \Sigma$ and the trace of $\Sigma = \tau - 1$.

A.2 Approximating Non-central Chi-squared Distribution by Normal

The following result can be found in [18, Chapter 29.10].

Theorem 7. *Let X be a random variable following a non-central chi-square distribution with ν degrees of freedom and non-centrality parameter δ, i.e., $X \sim \chi^2_\nu(\delta)$. Then the standarized random variable*

$$\frac{X - (\nu + \delta)}{\sqrt{2(\nu + 2\delta)}}$$

approximately follows a standard normal distribution if either

1. *$\nu \to \infty$, δ remaining constant, or*
2. *$\delta \to \infty$, ν remaining constant.*